NOTE

This Microfiche meets the quality requirements of the American National Standard for Microfiche of Documents (ANSI PH5.9-1975). However, because of imperfections in the document from which it was made, it contains images that are illegible or difficult to read. The source document for this microfiche is the best copy that could be obtained prior to filming.

CIS Congressional Information Service, Inc.
Washington, D.C.

DATA SECURITY SYSTEMS, INC.

COMPUTER SECURITY CONSULTANTS 5 Keane Terrace, Natick, MA 01760 (617) 653-7101

FEDERAL COMPUTERS AND TELECOMMUNICATIONS: SECURITY AND RELIABILITY CONSIDERATIONS AND COMPUTER CRIME LEGISLATIVE OPTIONS

DR. SANFORD SHERIZEN

NATICK, MASSACHUSETTS

A FINAL REPORT FOR THE OFFICE OF TECHNOLOGY ASSESSMENT

CONTRACT U.S. 433-0275.0

FEBRUARY, 1985

This contractor document was prepared by an outside contractor as an input to an ongoing OTA assessment. It does not necessarily reflect the analytical findings of OTA, the Advisory Panel, or the Technology Assessment Board.

J952-48

EXECUTIVE SUMMARY

Computers and telecommunications systems have become an important part of how Government operates, contributing to the efficiency and effectiveness of the Federal Government. The growth of these technologies has been rapid, even during the most recent periods of cutbacks and other efforts at cost containment. Predictions are that there will be a further growth, with more operations becoming computerized and more employees becoming information processors.

There has been a long history of Congressional concerns with topics which affect or are affected by this computerization. Basic issues such as privacy, crime, delivery of Governmental services, efficient use of Federal resources, and national security are related to the computerization, although the nature of the relationship is not well known.

The Office of Technology Assessment was requested by the Congress to prepare a report on a series of topics. This present paper is one of those reports. This paper concentrates on two major topics:

THE ADEQUACY OF SECURITY AND RELIABILITY POLICIES OF THE FEDERAL GOVERNMENT

COMPUTER CRIME TRENDS AND LIMITATIONS TO LEGISLATIVE RESPONSES TO CURRENT AND FUTURE TECHNOLOGICAL DEVELOPMENTS

A review was made of a variety of information sources, both

in the Government as well as in the private sector. Information was collected on past Federal Government efforts in these areas and an analysis made of the potential policy considerations and options of interest to the Congress.

Among the many individuals who provided information and assistance were Fred Wood, Jim Dray, Priscilla Regan and Jennifer Nelson of the OTA staff, Donn Parker of SRI International, Stanley Kurzban of IBM, Dr. Carl Hammer, Robert Brotzman and Shiela Brand of NSA, Eugene Epperly of DoD, Ed Springer of OMB, Lynn McNulty of State, Russell Rice of NASA, Richard Guilmette of Prime Computer, Richard Solomon of International Networks, Joseph B. Tompkins of Sidley & Austin, Gail Shelton of IG, HHS, Ned Saltzberg of Bigelow and Saltzberg, David Geneson of the U.S. Attorney's Office, District of Columbia, John D. Thomas of the Justice Department, Roger C. Adams of the Justice Department, Daniel R. Burk of Thomas & Fiske, Roy Freed of Brown, Rudnick, Freed & Gesmer, Fred Tompkins of MITRE, Steve Josselyn of International Data Corp, Walter Anderson of GAO, and Bob Harris of Congressional Budget Office.

HIGHLIGHTS OF THE REPORT

The United States Government has been involved with the security of communications systems since at least World War I and with computer security since the early days of computer developments. While much of this early interest was within the military and intelligence communities, recent developments in computers and telecommunications have led civilian agencies to become concerned with information security. Among the more significant of these recent activities responsive to the security implications of technology are:

1. National Security Decision Directive (NSDD) 145, dated September 17, 1984, is the latest basic policy document for the U.S. in the Information Age. It establishes mechanisms for an increased effort to protect national security-related information and places NSA in a leadership role in defining computer and telecommunications security in both military and civilian Government agencies.

2. OMB is currently revising Circular A-71, Transmittal Memo No. 1, which was first issued in 1978 to require Federal agencies to control and audit computer applications. This revision is in response to changes in technology and usage patterns, limited compliance by agencies, and negative reports on OMB's leadership in this security area.

3. DoD is seeking built-in multilevel computer security, with Trusted Computer Systems commercial products being evaluated, hardware and software standards being developed, and certification assistance offered to developers. This may result in some form of interagency cooperation.

4. NBS has undertaken a program to develop a guideline for Federal security certification that is an evaluation process assessing the extent to which a system or application satisfies Federal, agency, and user computer security needs.

5. The Inspector General of HHS led an investigation of computer fraud and abuse as part of the President's Council on Integrity and Efficiency. The report, released last year, was highly critical of Federal agency controls and the lack of detection mechanisms.

6. The Computer Fraud and Abuse Act of 1984 was passed in the last session of Congress and at least two separate indictments have been handed down charging individuals with violating the Act by illegally accessing Federal Government computers. The Administration has proposed the Federal Computer Systems Protection Act of 1984 as its long awaited computer crime bill and several computer crime bills have been presented during the early stages of the new Congressional session.

7. NSA, in a rare public statement, suggested to the Congress that U.S. advantages in advanced technologies, including development of nuclear weapons, are threatened by the poor security of the nation's communications networks. They recommended that a single agency supervise the development of communications security procedures, the carrying out of personnel security programs, and the purchasing of telecommunication security equipment, including some 500,000 "spy-proof" phones.

8. The Administration's proposed 50% funding cut for NBS' Institute for Computer Science and Technology may result in the elimination of a major center for computer security resources used both by civilian Government agencies as well as the private sector.

These and other activities within the Government represent fundamental considerations relevant to Congressional priorities. The indications that there are serious risks and vulnerabilities associated with current technology require consideration on the highest levels of Government.

MAJOR INFORMATION SECURITY ISSUES

The increased computerization of Government operations has led to a number of potential security problems. The dependency of Governmental services on reliable equipment and the growing

number of users who have the capability of unintentionally or intentionally misusing computers are just two of the more evident areas with security implications. A review of information security requirements in the Federal Government, contained in fuller detail within the text, leads to the following list of major information security issues:

- SECURITY HAS TENDED TO BE AN AFTERTHOUGHT IN THE DEVELOPMENT OF TECHNOLOGY AND THE IMPLEMENTATION OF INFORMATION RESOURCE MANAGEMENT.

- THE PRESENT STATE OF FEDERAL GOVERNMENT INFORMATION SECURITY IS A MUDDLE, WITH POLICIES AND PROCEDURES SUFFERING FROM PIECEMEAL DEVELOPMENT, A LACK OF CENTRAL LEADERSHIP, INSUFFICIENT ATTENTION AND RESOURCES FROM AGENCIES, AND LIMITED TECHNICAL TOOLS.

- ESSENTIAL INFORMATION FOR DETERMINING THE RISKS AND VULNERABILITIES OF COMPUTERS AND TELECOMMUNICATIONS SYSTEMS ARE NOT EASILY OBTAINABLE AND RISK ANALYSIS APPROACHES CONTINUE TO HAVE SERIOUS METHODOLOGICAL LIMITATIONS.

- COMPUTER CRIME HAS BECOME A SERIOUS NATIONAL PROBLEM AND THERE IS A GREAT POTENTIAL FOR FUTURE INCREASES IN OPPORTUNITIES FOR SUCH CRIME AND FOR MORE PROFESSIONALIZATION OF COMPUTER CRIMINALS.

- THE MERGING OF COMPUTER AND TELECOMMUNICATIONS SYSTEMS REQUIRES NEW EFFORTS TO DETERMINE POINTS OF VULNERABILITIES AND THE MEANS OF COORDINATING COMPUTER AND TELECOMMUNICATIONS SECURITY PROGRAMS.

- THE CURRENT RANGE OF SECURE INFORMATION PROCESSING EQUIPMENT IS LIMITED AND WILL LIKELY CONTINUE AS SUCH UNLESS CONCERTED EFFORTS ARE UNDERTAKEN BY THE FEDERAL GOVERNMENT TO SUPPORT SECURITY RESEARCH AND DEVELOPMENT, EITHER WITHIN THE GOVERNMENT AND THE PRIVATE SECTOR.

- THE NSDD 145, WHICH IS THE LATEST ATTEMPT TO MEET THE GOVERNMENT'S NEED FOR INFORMATION SECURITY, MAY CONTAIN FUNDAMENTAL CHANGES IN THE RELATIONSHIP BETWEEN THE CIVILIAN AND MILITARY AGENCIES OF THE GOVERNMENT.

- MANAGEMENT CONTROLS AND OTHER "HUMANWARE" ISSUES TEND TO RECEIVE LESS RESEARCH AND DEVELOPMENT ATTENTION THAN DO TECHNICAL APPROACHES.

MAJOR POLICY CONSIDERATIONS AND OPTIONS FOR THE CONGRESS

It is evident from this list that there are some fundamental information security and computer policy issues appropriate for Congressional consideration. These fall into the following policy areas:

1. GOVERNMENTAL RESPONSES TO COMPUTER CRIME. The potential for serious computer crimes against the Government as well as private sector information systems appears to offer major challenges to the limited security resource and prevention efforts. The near future expansion in the extent and nature of computer crimes suggest the need for concerted efforts to control the problem. Among the major policy considerations are:

COMPUTER CRIME LEGISLATION which includes (a) making no changes in existing laws but requiring law enforcement agencies to treat this as a priority area, (b) revision of existing laws and regulations to more specifically cover computer crime problems, (c) creation of new legislation as a "clean slate" approach specifically relating to computer crime, and (d) creation of legislation which includes computer crime as part of a larger coordinated information technology legislative review.

COMPUTER CRIME DETECTION AND PREVENTION is at a primitive level of development and there are relatively few individuals capable of providing service to agencies. Very basic work on developing detection approaches is required before agencies will be able to support Federal information security efforts. Among

the options available to the Congress are (a) supporting, requiring, and/or funding basic research on critical computer crime problems, (b) mandating more extensive agency prevention, detection, and reporting efforts, (c) designating a lead agency for detection and investigation efforts, and (d) encouraging computer and telecommunications manufacturers to strengthen access controls and other forms of security.

2. FEDERAL GOVERNMENT ORGANIZATION FOR INFORMATION SECURITY. The variety of technologies involved and the unprecedented types of problems raised may require new organizations and efforts to establish appropriate Federal Government information security efforts. Among the major options available to assist in this organizing for security are (a) requiring coordination or centralization of information security responsibilities, (b) establishing the means to overcome the implementation obstacles to agency information security efforts, (c) evaluation of NSDD 145 as a leading current policy document concerning the organizing of information security, and (d) inquiring about the reliability of Government information systems and the potential threats of overdependence.

3. MICROCOMPUTER SECURITY. The rapid increase of microcomputers within the Federal Government has led to special security problems. The microcomputer environment has several distinct characteristics which differentiate it from other forms of computer systems. These characteristics have created an

increased security problem for the Government, adding to the complexity of improving information security. Among the options available to meet this issue are (a) requiring security considerations to be incorporated within agency microcomputer purchase plans, (b) setting of standards for how security might require limitations on microcomputer configurations and usage patterns, (c) supporting the development of microcomputer security product evaluations and models for improved security awareness and training efforts by agencies, and (d) increasing end user security responsibilities and protections.

4. INFORMATION SECURITY RISK MANAGEMENT AND RISK ANALYSIS

Both risk management and risk analysis are required in information security programs in order to identify, evaluate, and respond to potentially serious problems affecting information systems. Congress can provide assistance in creating agency interest and active attempts to limit risks. Among the options are (a) requiring that risk analysis be incorporated within the early phases of system development and (b) supporting the transfer of risk analysis knowledge and techniques developed for other aspects of Government use.

The information and assortment of policy options found in this report provide the Congress with a menu of choices in strengthening the nation's information security. Previous Governmental efforts to establish information security have been found wanting. The success of future information security efforts will largely depend upon how Congress is able to grapple with quite complex technical and human behavior issues and to provide direction to Federal agencies as well as the nation at large.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

I. INTRODUCTION TO INFORMATION SECURITY 1

DEFINING COMPUTER CRIME

II. TECHNICAL DEVELOPMENTS AND IMPLICATIONS FOR SECURITY 11

COMPUTER DEVELOPMENTS AND SECURITY PROBLEMS

III. RISK MANAGEMENT AND RISK ANALYSIS 17

RISK MANAGEMENT AS A FEDERAL GOVERNMENT CONCERN

RISK ANALYSIS

PROBLEMS ASSOCIATED WITH RISK ANALYSIS

AN OVERVIEW OF RISK ANALYSIS

MAJOR RISK ANALYSIS APPROACHES

IV. FEDERAL SECURITY AND RELIABILITY POLICIES 41

A HISTORY OF FEDERAL SECURITY AND RELIABILITY POLICIES

AN OVERVIEW OF STAKEHOLDERS IN INFORMATION SECURITY

V. THE DUAL NATURE OF INFORMATION SECURITY 53

A BRIEF HISTORY OF COMMUNICATIONS SECURITY IN GOVERNMENT

A BRIEF HISTORY OF COMPUTER SECURITY IN GOVERNMENT

VI. THE PRESENT STATE OF GOVERNMENT INFORMATION SECURITY 61

NATIONAL SECURITY DIRECTIVE 145

ANALYSIS OF NSDD 145

VII. PROBLEM ISSUES IN INFORMATION SECURITY 75

OBSTACLES TO INFORMATION SECURITY IMPLEMENTATION

BALANCING PREVENTION AND PRODUCTION AS COMPETITIVE REQUIREMENTS

VIII. COMPUTER CRIME LEGISLATION 82

FACTORS AFFECTING THE DEVELOPMENT OF COMPUTER CRIME LAW

FEDERAL LAWS APPLICABLE TO COMPUTER CRIME

HISTORY OF FEDERAL COMPUTER CRIME LEGISLATIVE EFFORTS

CRITICISMS OF PAST COMPUTER CRIME LEGISLATION

CURRENT LEGISLATION AS OF THE END OF THE 98TH SESSION

THE ADMINISTRATION'S PROPOSED LEGISLATION

VIX. A DEVELOPMENTAL MODEL OF FUTURE COMPUTER CRIME 101

FACTORS AFFECTING FUTURE COMPUTER CRIME DEVELOPMENTS

TECHNICAL DEVELOPMENTS AND POSSIBLE COMPUTER CRIMES

MODES OF LEARNING ABOUT COMPUTER CRIME

PROFESSIONALIZATION OF CRIMINALS

EVOLUTION OF SPECIALIZED CRIMINAL SKILLS

PUBLIC RESPONSE TO COMPUTER CRIME

COMPUTER CRIME COST-BENEFIT CONSIDERATIONS

X. PROBLEM ISSUES IN RESPONDING TO COMPUTER CRIME 118

DIFFICULTIES IN THE DEVELOPMENT OF TECHNOLOGICALLY RELEVANT LAW

MAJOR EVENTS IN THE INVESTIGATION AND PROSECUTION OF A COMPUTER CRIME

ESTABLISHING APPROPRIATE LEGAL RESPONSES AND ALTERNATIVE STRATEGIES FOR CONTROLLING CRIME

XI. POLICY PERSPECTIVES ON INFORMATION SECURITY AND COMPUTER CRIME 125

GOVERNMENT RESPONSES TO COMPUTER CRIME

COMPUTER CRIME LEGISLATION

OPTIONS

COMPUTER CRIME DETECTION AND PREVENTION

OPTIONS

FEDERAL GOVERNMENT ORGANIZATION FOR INFORMATION SECURITY

OPTIONS

MICROCOMPUTER SECURITY

OPTIONS

INFORMATION SECURITY RISK MANAGEMENT AND RISK ANALYSIS

OPTIONS

FOOTNOTES 147

INFORMATION SECURITY

I.INTRODUCTION TO INFORMATION SECURITY

There are now more computers in the world than there are people, if the computers in a chip are counted. In a relatively short period of time, a technological revolution has occurred, creating changes in every institution of our society and creating new forms of behavior which are still undergoing evolution.

One important consequence of this computer/ telecommunications revolution is the creation of a new crime. Computer crime, only possible with the advent of the computer, has become a well known aspect of the Information Age. Government and businesses are victims of crimes which become covered by television, highlighted in movies, and trumpeted by the news media. Despite this intensive coverage, however, computer crime suffers from certain sterotypes which detract from its importance. The mass media portray computer crime in sensational terms, emphasizing the crimes while ignoring the protections that exist to guard against such acts. Security is a tainted word, conjuring up images of police tactics and invasion of privacy. Many managers, even those with data processing backgrounds, find it difficult to pinpoint the kinds of data that can be stolen from their computer systems and how these acts might be committed.

The computer mystique encourages some people to have blind faith in computer-generated information. The suspicious manager, who reviews financial transactions in a manual setting, may not adquately review the operations that affect information generated

by a computer. Indeed, the complexity of computers, with their own sets of esoteric operations and jargon, leads many managers to suspend usual checks and balances, allowing data processing technical staff more freedom to access and manipulate information than might be desirable or necessary. [Sherizen]

Government tends to be one of the major victims of computer crime, both because it has undergone such rapid computerization without adequate safeguards against crime as well as the fact that fraud has been a large scale problem, even in the pre-computer age. [Comptroller General of the United States, AFMD-81-73] Basic Government services are highly dependent upon computers and telecommunications, causing what could be an overdependence upon information processing without adequate security or reliability measures. Essential citizenship issues, such as privacy, confidence in Government, integrity of public servants, and the protection of national security information are dependent upon the ability of the Government to ensure safe and secure operations.

The problem of computer crime is thus not simply media hype but potentially fundamental to the continuity of Government as well as private sector institutions. The materials that follow will discuss the nature of the computer crime problem and indicate some of the more problematic features of this complex issue.

Defining Computer Crime

As computer crime has become more of a national problem, it has become evident that the term has many different meanings. The media in particular have used computer crime to cover a range of actions, ranging from financial fraud using a computer to someone physically attacking a computer. There are, however, several definitions which have come to be accepted by experts in the field. Whether called computer crime, computer abuse, or computer-related crime, it involves an illegal act for which knowledge of computer technology is essential for its perpetration and prosecution. [**Computer Crime: Criminal Justice Resource Manual**] Senator Ribicoff's bill (S240) identified four main categories of computer-related crime:

> the introduction of fraudulent records or data into a computer system
>
> unauthorized use of computer-related facilities
>
> the alteration or destruction of information or files
>
> the stealing, whether by electronic means or otherwise of money, financial instruments, property, services, or valuable data.

The President's Council on Integrity and Efficiency study [Kusserow] defined computer-related fraud as:

> any illegal intentional act or series of acts that is designed to deceive or misrepresent in order to obtain something of value. Further, a computer system must have been involved in the perpetration or cover-up of the act, or series of acts. A computer system might have been involved through improper manipulation of: (1) input or transaction data, (2) output or results, (3) applications programs, (4) data files (5) computer operations, (6) communications, or (7) computer hardware, systems software, or firmware.

The Council added a definition for computer-related abuse which is:

> the misuse, destruction, alteration or disruption of data processing resources. The key aspects of computer-related abuse are that it is intentional and improper, but it does not necessarily imply the violation of a specific law nor the presence of false representation. Examples of computer-related abuse are (a) unauthorized use of the computer by Federal employees for their personal programming activities, and (b) misuse of computer equipment for revenge against a government agency.

More formal legal definitions of computer crime and abuse are to be found in the section containing a discussion of computer crime legislation.

Examples of computer crime against Government operations are plentiful. Among those mentioned in the PCIE study are:

> A Federal employee, through access to benefit claims authorization and input procedures, fraudulently obtained over $100,000 over 1 and one half years. He used the computer to reactivate accounts of deceased beneficiaries, and to create fictitious records. The case was detected by a bank clerk who observed the perpetrator opening more than one direct deposit account (in different names) at the same bank. The bank reported the observations to Federal officials.
>
> A Federal employee was able to establish unauthorized benefit claims and divert $24,000 over a 5-month period. The perpetrator was able to change information in a deceased client's file and correct his input errors because no segregation of duties existed in the edit resolution so his corrective inputs were not reviewed by a supervisor. After a check was generated, the perpetrator was able to erase erroneous data. Eventually the case was detected by a computer match and subsequent investigation.
>
> Another Federal employee was able to override input controls and redirect program recoveries to his own bank account. The perpetrator was able to clear a systems alert code, delete a notice of recovery, and steal the repayment. There was no system of review to assure proper posting of recoveries. This fraudulent act went undetected until a fellow employee accidently noticed the improper processing of cases and notified management.

A caseworker created fictitious applications for Food Stamps. She entered the fictitious information in the computer to generate authorizations to purchase Food Stamps, which she then received and cashed. Although there were procedures to assure supervisor review of new applications and authorization of new transactions, the procedures were not followed. The case was detected accidently by a co-worker. The estimated loss in the case exceeded $12,000.

Three data entry clerks were able to steal Food Stamps, valued at over $150,000, because the supervisor consistently left his key in the issuance terminal. The clerks stole the Food Stamps and used the computer to generate false issuance reports by deleting their personal "transactions" from the file. Written procedures requiring authorization of transactions, management review, and input controls were not used by the supervisor. The supervisor's failure to control access to the issuance terminal also violated agency policy.

These cases are but a few examples of a large number of computer crimes found both in the Government as well as in the private sector.

Criminologists and other experts have determined certain patterns in computer crime [Sherizen]:

1. Losses from computer fraud and abuse are estimated to be quite high, although experts have not been able to make accurate estimates.

2. It is estimated that relatively few computer-related crimes are every detected and only a minimal chance that those detected will be prosecuted.

3. Computer criminals can be motivated by a variety of reasons, including money, revenge, challenge, and ideology.

4. Computer crimes may occur over a long period of time and often are discovered by accident, tips from disgruntled spouses or fellow employees, or the perpetrator's own bragging. Relatively seldom are they discovered by security or audit personnel.

5. Trusted inside personnel may be more inclined to commit these acts than are outsiders because they have greater opportunity. But there does appear to be an increasing amount of collusion, often between inside personnel with access to equipment and outside persons with technical knowledge.

6. Some computer crimes are committed by people with highly sophisticated technical knowledge, although those with minimal computer literacy, working in environments with lax management controls, also commit these crimes.

Computer crime tends to have certain characteristics which differentiate it from more traditional crimes. Many who consider committing computer crime realize that systems are inadequately protected; possibility of detection is slight; risk of being caught is minimal; crime evidence may not exist if audit trails are not created or followed; and punishment is rare, even if one is caught, since few companies, and possibly agencies, are willing to press charges. Talk about temptation!

Because computer security is inadequate in many offices, opportunities for computer crimes are found easily. Few managers realize how vulnerable their systems are and how easily sensitive assets could be compromised. With the growth in the use of microcomputers and networks, opportunities for crime have increased while controls over fraud and abuse have diminished. Rapid changes in technology will probably cause this trend to continue unless computer security measures are instituted.

It is easy to ignore the illegality of computer crimes. After all, they do not involve bloodletting, carrying a weapon, or direct contact with the victim, which often turns out to be an organization rather than an individual. A person comitting an illegal act can profit without having to leave the office or to modify his or her role as a good citizen.

Finally, personnel who use computers in their work often discover weak points in the system that could be bypassed for personal gain. But one does not need to be an insider to acquire

such information since electronic bulletin boards often contain information about access codes, passwords, and methods used to bypass certain security protections.

These characteristics can be summarized, as shown in the following exhibit.

CHARACTERISTICS OF COMPUTER CRIME

Requires Minimal Risks for Major Gain

Opportunities are Readily Available

Those Who Commit These Crimes May View Their Acts As Non-Crimes

Information on How to Commit Computer Crimes is Easily Available

Three recent studies of computer crime provide basic information on the problem. The first was undertaken by the interagency task force of the President's Council on Integrity and Efficiency (PCIE), headed by Richard Kusserow, the Inspector General of HHS. This June, 1983 report is entitled **Computer-Related Fraud and Abuse in Government Agencies.** Another recent study was performed by the Task Force on Computer Crime, Section of Criminal Justice, American Bar Association. The study was headed by Joseph B. Tompkins, Jr. and released in June of 1984 under the title, **Report on Computer Crime.** The final report to be discussed is entitled **Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries.** It was established by the EDP Fraud Review Task Force of the American Institute of Certified Public Accountants in 1984.

While there are methodological issues with these studies, they provide support for a number of contentions made by earlier research studies and give an overview of the problem of computer crime and abuse. Major aspects of the findings are:

> Perpetrators employed a variety of schemes, methods, and techniques. Relatively few of these were sophisticated, many simply being easily committed input changes.
>
> A majority of the cases involved only one perpetrator and they tended to be employees within the organization rather than outsiders penetrating their systems.
>
> Losses per case covered a large range, with some quite minimal to, in some reported cases, several million dollars. Total losses were estimated to be quite sizeable, with the ABA reporting that over 25% of their respondents indicated known and verifiable losses due to computer crime during the last month falling between $145 million and $730 million. Multimillion dollar losses were not uncommon in this sample of organizations.

> Few organizations appear to have put into place the means to detect computer crime or to estimate the value of their computer crime losses.
>
> In a number of cases, sometimes over half of the total, detection was by accident, such as nonroutine events, unusual activity of the perpetrator, or tips. Many fewer incidents were detected through traditional internal controls. Security and auditing personnel found a limited percentage of the cases which came to the attention of management.

These findings indicate that many of the traditional rules which managers followed in the pre-computer age may not be sufficient for the prevention of computer crime. The new world of technology requires new rules for security. Traditional physical security approaches are not sufficient. Microcomputers are able to penetrate systems unless virtually costless controls to prohibit retrying of passwords at electronic speeds and to prevent penetrations of the types widely reported are put into place. The rules have changed, with security now the responsibility of many managers who previously had little interest or need to be involved with these problems. In essence, security has become a major managerial problem requiring mangerial controls and supervisory activities to protect computerized assets. How security became such an important aspect of technology requires a brief historical overview, which is provided in the following section.

II. TECHNICAL DEVELOPMENTS AND IMPLICATIONS FOR SECURITY

Yesterday's technical development is today's security problem. Technological advancements have been oriented toward faster, more efficient, and more effective operations rather than security complications resulting from these developments. Since security has often been an afterthought or the concern of security specialists who played a relatively minor role in development, technological advancements did not have a security focus. The end result has been that security concerns have tended to develop after individuals have used the technology in ways different than perceived by the developers. Generally, only well after security problems have developed is there an effort undertaken to develop security mechanism, which often tend to be measures which are added on rather than built into the technology.

This difference in development rates creates time lags in the evolution between security and technology. This can be seen in the following chart, which describes the major computer generations and the security complications associated with each generation. [Adapted from Tangney, Edwards]

COMPUTER DEVELOPMENTS AND SECURITY PROBLEMS

Major Technical Features of System

First Generation (Mid 1940's-circa 1960):

- Vacuum tube-controlled circuitry
- Single user systems with no resource sharing.
- Programmer was operator.
- No operating system as presently known
- Limited storage

Second Generation (1960-circa mid 1960's):

- Transitional period
- Solid state circuitry
- Advent of operating system software (monitor)
- Specialization between system and application programmers
- Single user at a time batch processing
- Beginning of time sharing and information processing
- Increased speed and reliability

Third Generation (1964-circa 1970):

- Multiprogramming
- Solid state integrated circuits
- General purpose computing systems
- Operating systems
- Batch systems
- Numerical computering and information processing
- Instruction set compatability
- File systems
- Increased user demand
- Emphasis upon full use of resources

Current Generation (1970's-present):

- Multiprocessing
- Mini and microcomputers
- Large scale integrated circuits
- Timesharing
- Program concurrency resident in main memory
- Virtual memory architectures
- Operating system with security features
- Per-process virtual environment
- Increased storage
- Communications linkages and integration
- Increased special applications

Major Technical Protection Problems

First Generation:

User had access to all physical and internal resources
Inadvertent destruction of software
Existing security was mainly at data source and end use

Second Generation:

Same as first generation
Protect resident monitor programs from resident user programs

Third Generation:

Concurrent multilevel use and processing
OS shared resources among several resident user programs
More than one user program in main memory at time
Protection resources managed by OS

Current Generation:

Isolate processes yet permit controlled sharing
Hardware and software to support secure multiprocessing
Protecting one user process from another
Protect OS software from user process
Protect system resources from user processes
Microssingle state machines with no supervisory state

Major Technical Protection Structures

First Generation:

Single user programs
No resource sharing
Classified or protected sites
Classified personnel
System protected at high security level
Security controls often external to applications

Second Generation:

Separation of applictions from systems areas
System and user at highest levels of security
Hardware to protect resident monitor software

Third Generation:

Memory protections
CPU and I/O protections
Two-state processor
Software protections
Privilege instructions
Audit logs

Current Generation:

Virtual memory architecture
Execution domains
Hierarchical domains
Concentric Circles
I/O access controls
Passwords
File system access controls
Audit mechanisms
Encryption

Continuing Technical Security Problems

First Generation:

Relatively protected for that time and place

Second Generation:

Users had access to most resources
Equipment moving out of protected environments
Low classified materials had to be manually declassified

Third Generation:

O.S. unreliability
O.S. could be subverted to undercut hardware protections
Increasing number of applications with new users
Mixtures of information classifications and security needs

Current Generation:

O.S. still unreliable from a security perspective
Multileveluses may not be secure for sensitive environs.
Traditional security techniques being used
Variety of penetrations possible
Built-in security rather than add-on security tradeoffs
Lack of centralized policy and procedures controls
Coordinationneeded for computer & communications security

As should be evident from this chart, there are serious security problems existing with contemporary computer systems. Added to this is the fact that the 1980's have seen a tremendous spread of networks linking up widely distributed computers and terminals, ranging from local area networks within a single agency to world-wide public and private networks. The same

network may support hundreds of users simultaneously, each with different access rights to data and programs within the larger system. The security problems of facilitating desirable sharing of programs and data while protecting them against misuse is one of the most complicated tasks facing the Government. How to approach this problem is discussed in the following section.

III. RISK MANAGEMENT AND RISK ANALYSIS

Contemporary life is filled with the need to make decisions about risks and losses. A disaster in India which is based upon high technology processes, decisions on how deregulation should proceed on the Federal level, determinations of how the possibilities of cancer causing additives should affect the food industry, and release methods for new drugs are just some of the types of considerations which affect Government today. Techniques to estimate the potential risks and losses have been a mainstay of the insurance industry operating as a basic ingredient in the decisions on premium rates. This methodology has more recently been adopted by other industries in need of some estimates of risks and applied to a variety of subject areas, including that of information security in Government.

The wide interest in risk analysis, sometimes also called risk assessment, is demonstrated by several developments, including [Lawless, et al.]:

> A ten-fold increase in risk assessment studies published in professional journals and discussed at scientific symposia in the 1960 to 1970 period
>
> The establishment of a number of new Federal and state agencies directed to deal with specific risks.
>
> Since 1979, the Congress has annually considered a bill to promote research on and systematic application of improved formal risk assessment methods by Federal agencies. In 1982, the House passes HR 6159, the RISK ANALYSIS RESEARCH AND DEMONSTRATION ACT, but the Senate did not take action on its version.
>
> The National Science Foundation has an active program on risk assessment, resulting in the publication of a number of scientific reports and evaluations.

Risk Management as a Federal Government Concern

Risks are a normal feature of management, whether in the Government or in the private sector. Managers have to maintain a balance between various pressures, planning for the short as well as the long term. In the past, most managers have tended to view crime-related risks as low priorities, particularly when the losses were minor and security personnel could be given responsibility for crime control efforts. With the increased computerization in the Federal Government and the issuance of regulations such as A-71, the importance of risk management has increased. Managers are being required to review the ways by which their computerized assets and resources are protected, determine the adequacy of protections, and plan protective programs.

There are certain basic risk management approaches that may reduce risks in computer operations. Four of these management options are:

1- RISK AVOIDANCE. Risks may be avoided by removing vulnerabilities or assets, especially those related to sensitive operations. Encryption of vital data flowing over communications lines offers one means of limiting unauthorized access.

2- RISK ABATEMENT. Even when risks cannot be eliminated completely, because of technical and/or operational factors, controls can be implemented to lessen these risks. For example, increased auditing controls and monitoring efforts can provide risk control without unduly interrupting normal work operations in an agency.

3- RISK CONFINEMENT. In certain environments, risk may be mitigated by transferring centralized data-processing tasks to different decentralized units or to other responsible parties, such as insurance companies. This division of tasks involves less risk than centralization of all processes.

4- RISK ASSUMPTION. Management may decide to accept the risk and the consequences of a loss when the cost of the loss is not significant (such as when replacing publicly available information is inexpensive), the cost of preventing or limiting it exceeds the potential loss (encryption for certain operations may not be cost effective), or the probability of a loss occurring is small (such as the theft of a mainframe).

These risk managment decisions should only be decided as part of a risk reduction decision process. The major steps involved in such a process are indicated in the following exhibit.

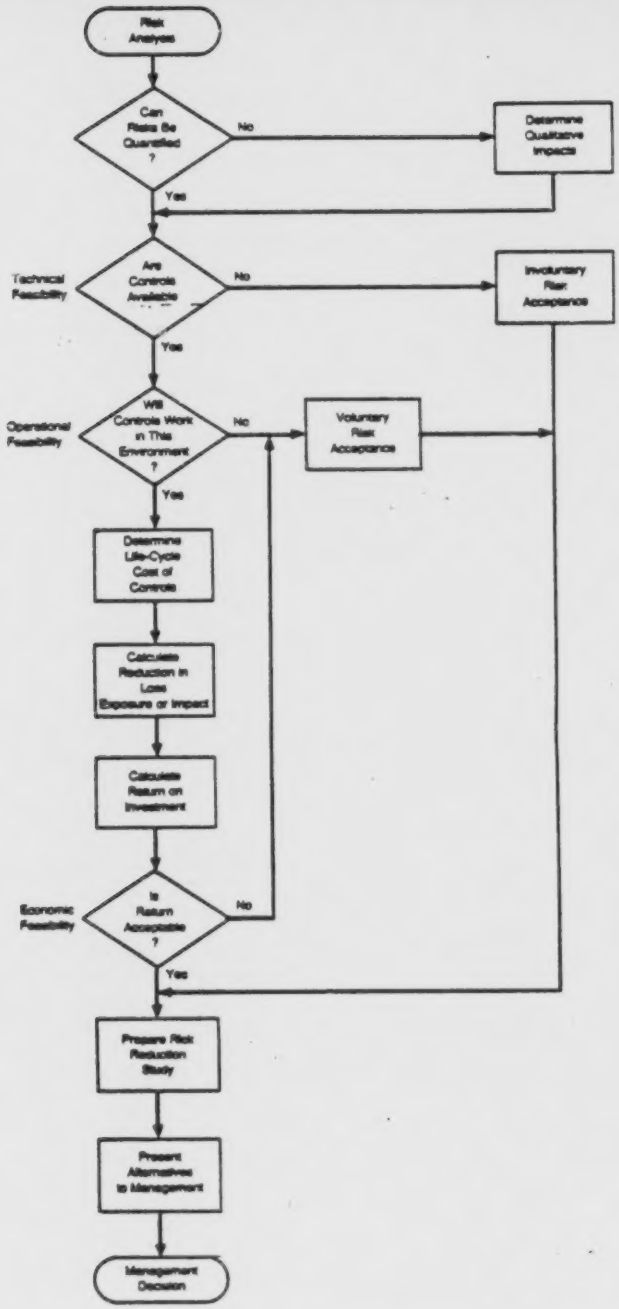


FIGURE
RISK REDUCTION DECISION PROCESS

(Thompkins)

RISK ANALYSIS

Computer and telecommunications systems are fraught with risks and vulnerabilities which can affect the Government's capability to deliver vital services, to protect sensitive personal and national secrets, and to guard against looting of the public treasury. While there has been widespread discussion about these problems, there has been relatively little success in pinpointing the potential for these problems to occur, determining how much security is sufficient, and motivating managers to undertake systematic security reviews. One technique which could provide some of the necessary information and has been developed as an analytical tool for examining these problems is risk analysis.

Risk analysis is a fundamental tool for determining the scope and direction of risk management efforts. It provides a baseline measure of the security problems and indicators of what potential safeguards and efforts can be established to counter losses.

Risk analysis has been defined in the National Bureau of Standards FIPS PUB 39 as an analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. It is a concept having a broader definition that that of risk assessment, encompassing risk assessment, risk reductions, and risk management.

A risk analysis is but one of a number of methods available for inspecting, testing, or evaluating security of systems. These include penetration attempts, vulnerability studies, security audits, checklists, and questionnaires. These may not, however, serve as a substitute for a full risk anaysis since only this approach considers the key elements of damage, likelihood of occurence, and/or cost of recommended controls.

Risk analyses can contribute to basic planning decisions and as such are required for certain Government agencies. Conducting a risk analysis:

1. gives guidance on the amount of resources to spend on each security measure and permits scarce resources (people, money, equipment) to be allocated where payoffs are highest.

2. alerts management to near-term risks with unacceptable economic, legal, political, social, or ethical consequences.

3. pinpoints the need for corrective actions.

4. directly relates objectives of the security program to the functions of the organization.

5. increases security awareness at all organizational levels.

6. results in criteria for designing and evaluating contingency plans for backup operation, recovery from a disaster, and ways to deal with emergencies. [Kittelberger]

While these are powerful contributions, there are also some major limitations to risk assessments. These are:

1. risk analysis deals with future events, making predictions of both loss and occurence rates extremely difficult, if not impossible, in some cases.

2. the information upon which the risk analyst bases predictions is imperfect.

3. no single methodology is broadly applicable to all risk managment environments since risk assessment is an analytical process with a large number of variables, many of which are unknown and unique to the environment under consideration.

4. costs for a full analysis can be quite high, depending upon the nature of the environment being reviewed. [Ibid]

These limitations are serious, raising questions on how important a role should be defined for risk analyses. At this time, for example, risk analyses are required under A-71 for each computer installation operated by an agency, including installations operated directly by or on behalf of an agency.

That Directive states that a risk analysis shall be performed (1) prior to the approval of design specifications for new computer installations, (2) whenever there is a significant change to the physical facility, hardware, or software at a computer installation, and (3) at periodic intervals of time established by an agency, commensurate with the sensitivity of the information processed by the installation, but not to exceed five years.(Section 4f)

Problems Associated With Risk Analysis

While there has been progress in developing new approaches to risk analysis, there are serious limitations which are evident regardless of advances in methodology. Three major problems are those related to (a) the risk analysis process, (b) changes in technology, and, (c) acceptance of risk analysis for strategic planning purposes. Each of these will be briefly discussed.

The risk analysis process is based upon unknowables and unpredicatables. It is one thing to spell out all of the possible factors involved in a threat and it is quite another to be able to predict when, how, how often, and in what fashion it can occur. Central to this problem is the fact that perceived risk and actual risk tend to be poorly correlated. This is a critical issue for risk analysis, since there may not be a sufficient knowledge base for actually predicting risks and the perception of the person making predictions of risk may be critical to determining final estimates.

An illustration of misperceptions is found in a study in the U.S. of non-experts' estimates of the causes of death from forty-one different causes. [As cited in Norman]

Estimations vs. True Probabilities of Causes of Death

CAUSE	ACTUAL	PERCEIVED	RATIO
Smallpox	0	57	---
Botulism	2	183	91
Fireworks	6	160	27
Smallpox vacination	8	23	2.9
Venomous bite/sting	48	350	7.30
Tornado	90	564	6.3
Homicide	18,860	5,582	0.30
Suicide	24,600	4,679	0.19
Diabetes	38,950	1,476	0.038
Vehicle accident	55,350	41,161	0.74
Stomach cancer	95,120	3,283	0.035
All accidents	112,750	88,879	0.79
Heart disease	738,000	23,599	0.032
All diseases	1,740,450	88,838	0.051

In general, rare events were perceived to be much more common, while common occurences were underestimated. Events that got reported but were not very rare, like accidents and homicide, were most accurately perceived. Interestingly, the public misperceptions of the magnitude of some risks were strikingly similar to the degree of newspaper coverage of these deaths. It is possible that these findings could be applicable to the problems of risk estimation in the risk analysis process.

There is also the growing sense that the risks and vulnerabilities involved with distributed systems and the integration of computers and telecommunications may be a much more complex set of risk analysis problems than earlier technical generations. The risks and vulnerabilities may be additive, with security problems accumulating in new and potentially dynamic fashion. An example of how complex risk analysis can be is shown in the following exhibit, which illustrates one assessment instrument and its relationship to various stages of a risk assessment.

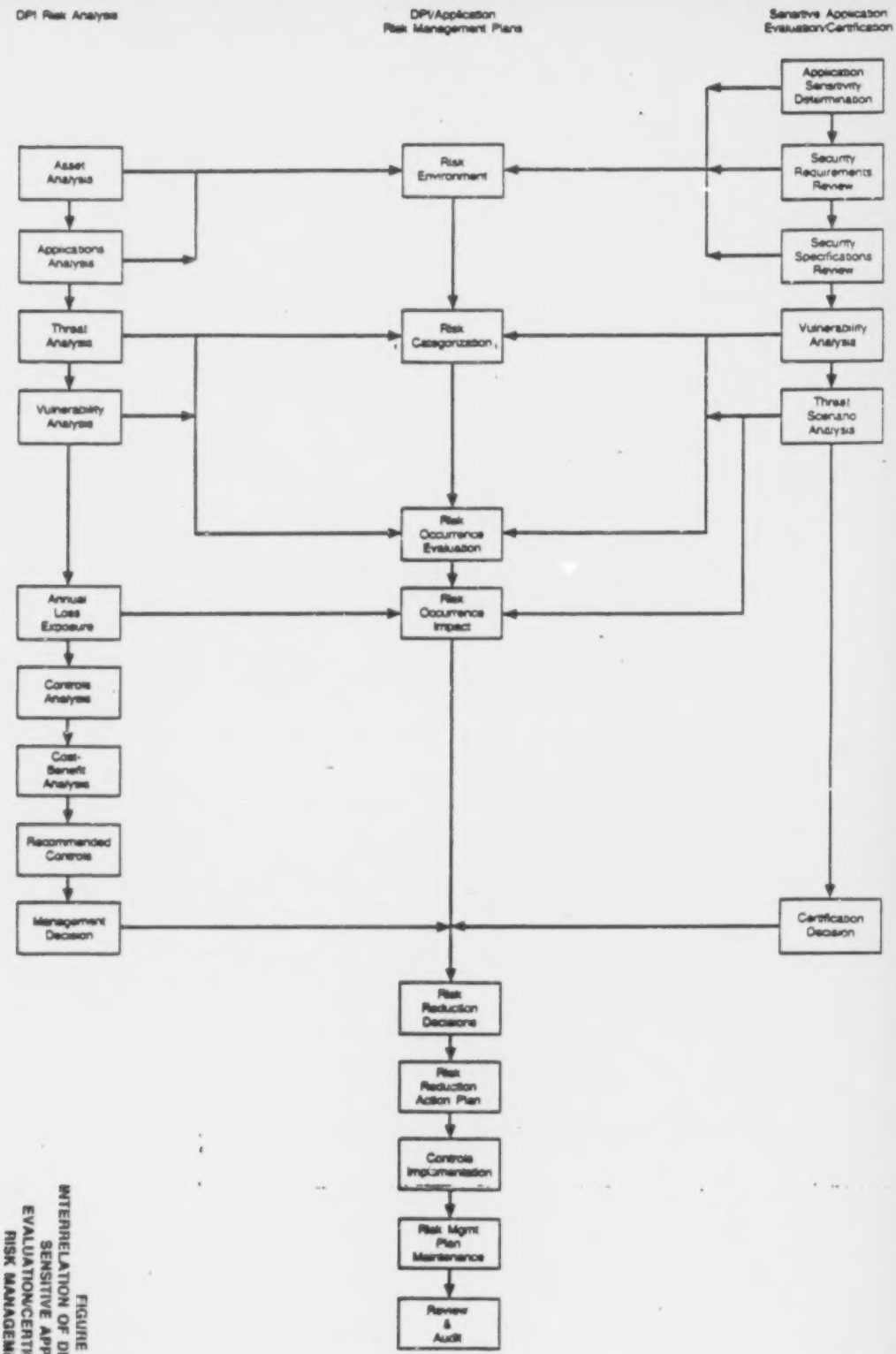


FIGURE
INTERRELATION OF DPI RISK ANALYSIS, SENSITIVE APPLICATION EVALUATION/CERTIFICATION AND RISK MANAGEMENT PLANS

(Tompkins)

A final major problem area is that the decisions to perform a risk analysis and the uses of the analysis are under the control of managers who may not accept its assumptions or its usefulness. It is a safe assumption that many risk analyses have been performed as an obligatory effort, with little agency interest beyond meeting the requirements. In some instances, the persons assigned to perform these required risk analyses have been those who bureaucratically are available rather than those who have the capabilities to make the estimates which are so crucial to accuracy of the analysis. In essence, there appear to be are very few well performed risk analyses and very few strategic decisions based upon the risk analysis process.

An Overview of Risk Analysis

A computer security risk analysis methodology contains at least six essential elements. These are:

1. A statement of the scope and purpose of the risk analysis. This should include information on the purposes and objectives of the exercise. Among the information included in this statement are:

Reasons for risk analysis

- Legal requirement
- Managerial information
- Insurance
- Auditing
- Periodic requirement

Objectives

- Measurement of possible risks
- Estimation of possible losses
- Determination of potential safeguards
- Quality Control

Responsibilities

Risk analysis team
Reporting requirements
Information to be collected
Cooperation expected
Guidance for estimations

Restrictions

Critical applications
Privacy protections
Time limited effort
Costs
Limitations

These are but indications of the types of information which can help to define the nature of the project and to inform those who will be involved as well as affected by the process.

2. An analysis of resources which are of value to the organization being studied and which may be susceptible to loss. Among the major categories of assets are [Carroll]:

EQUIPMENT

capital goods
support equipment
furniture and fixtures

INFORMATION

data
files and records
computer software

INVENTORIES

merchandise or supplies
work in progress
raw materials

NEGOTIABLES

cash
vouchers
checks
bills
policies
bonds

PERSONNEL

employees
clients
others

SERVICES

to the public
to other agencies
to employees

LEGAL LIABILITIES

injuries
errors and omissions
negligence
Privacy Act violations

Determinations should be made about what resources are most important for an organization, defined in terms of how critical it is to an organization's abilities (such as payroll or certain client services) or sensitivity (personal, proprietary, financial, or national security information). Decisions might have to be made about priorities to be evaluated first in their order of importance.

3. An analysis of threats whose occurrence could cause loss. Specific threats have been categorized into four major loss categories: damage, denial of possession, denial of use, and

disclosure. Other threat categories sometimes mentioned , such as delay, modification, and destruction, can be viewed as degrees or elements of the four major categories. A more specific listing of threats would include [Ibid]:

agent access
airborne particles
air conditioning failure
application program change
bomb threat
communications malfunction
communications outage
data alteration malfunction
data denial
data entry error
data entry (fradulent)
disgruntled employee access
earthquake
eavesdropping, wiretapping
electromagnetic interference
emanations interception
embezzlement
explosions
fire
floods
fraud
handling media improperly
hardware alteration
hardware denial
hardware malfunction
hurricanes
ice and snow storms
injury or death
landslides
lightening
liquid leakage
marking media improperly
mechanical shock/vibratn
misuse of resources
operating sys penetration
operating sys alteration
operator error
power outage, transient
Privacy Act violation
programming error
radio frequency interfer.
riot/civil disturbance
software denial
static elec discharge
strike
terrorist actions
theft
tornado
tsunami
unauthorized disclosure
unclear personnel access
vandalism
volcanic eruption

Threats tend to be categorized into natural hazards, accidental acts and intentional acts. All of these need to be noted in a review.

4. An analysis of vulnerabilities in security controls which might increase the frequency of threat occurrences and/or the impact of such occurrences. A list of these vulnerabilities would include the following [Ibid]:

inadequate or unreliable air conditioning, heating, ventilatn
applications software design weakness
insecure applications software development procedures
unstructured applications software design procedures
inadequate or nonexistent audit procedures or support
inadequate or nonexistent backup or off-site storage
inappropriate building construction
obsolete or inappropriate communications hardware
insecure or unreliable communications lines
obsolete or insecure communications software
insecure, unstructured, or nonexistent data management
insecure or nonexistent document control
intelligible acoustic or electromagnetic emanations
inadequate or nonexistent emergency planning/procedures
ineffective error detection and correction provisions
ineffective or nonexistent external physical access control
inadequate fire protection
inadequate or obsolete data processing hardware
inadequate housekeepping
insecure input-output procedures
ineffective or nonexistent internal physical access control
opportunities for liquid leakage
inappropriate geographical location
lack of management support for security
insecure or nonexistent media storage on-site
insecure, obsolete, or inappropiate operating system software
insecure or disorganized operating procedures
personal hazards in the workplace
incompetent, disloyal, or unreliable personnel
inadequate or unreliable electric power service
ineffective or insecure recovery and dp backup procedures
inadequate or nonexistent risk management
ineffective or nonexistent computer security organization
ineffective or nonexistent security procedures
inadequate or nonexistent security training/awareness program
no security orientation in software acceptance procedures
inappropriate software life-cycle and maintenance procedures
inadequate or nonexistent off-site storage
ineffective or nonexistent controls over supplies
obsolete or insecure system access provisions
obsolete, insecure, or ineffective terminal access provisions
inadequate or unreliable hardware maintenance

These vulnerabilities can also be categorized into (a) administrative types which includes security management, personnel security, procedural controls, and contingency planning (b) physical vulnerabilities which includes access control, environmental controls, and hazard protection, and, (c) technical vulnerabilities which includes hardware, operating system, application system, communications, and data base management systems.

5. A calculation of overall risks which quantitatively and/or qualitatively measures the possible losses to the organization being studied. It should be noted that in order to achieve this step, the previous steps in the process have had to be completed and been put into a form which allows for estimating total amounts of potential damage. Depending upon the accuracy of these earlier steps, this step in the process will be able to provide an estimate of the expected annual impact of each threat on organizational assets. This involves determining the estimated single-time loss for each threat identified within each area of exposure which has been ascertained. Once the destruction, modification, disclosure, and delay losses to each exposure zone from a threat have been determined, these should be added together in a manner which considers the possibilities of additive effects. Expected losses can be estimated by (a) impact area, (b) threat, (c) asset category, and, (d) vulnerability.

Various approaches have been taken to provide this calculation, with the major based upon some quantitative measure. The ALE or annual loss expectancy is most well known of these

approaches with fuzzy matrices or more qualitative approaches also available. A sample of an ALE matrix follows.

ALE WORKSHEET

(Dept. of Labor)

Page ___ of ___

THREAT: ANNUAL FREQUENCY ESTIMATE (AFE):
ORGANIZATION: PREPARED BY: DATE:
DIVISION: FORM NUMBER:
NOTE: Comments may be entered on reverse side.

ANNUALIZED LOSS EXPECTANCY

SINGLE LOSS ESTIMATE

DAMAGE

DENIAL OF POSSESSION

DENIAL OF USE

DISCLOSURE

REPLACEMENT VALUE

ASSETS

VULNERABILITY	LOCATION			LOSS CATEGORIES					
Intermediate Totals:									
Intermediate Totals:									
Intermediate Totals:									
D I V I S I O N T O T A L S:									

5. An analysis of security control measures which, if implemented, would act as safeguards in reducing threat occurrences and/or the impact of such occurrences. This involves decisions on those security controls which can recduce the occurence rates of a threat(s) and/or reduce the effects of a threat(s) once it has occurred. Among the major safeguards or countermeasures are: [Carroll]

Organizational Measures

- management support
- financial support
- security officers
- security training and awareness

Security Administration

- clearance/classification system
- storage of high-risk material
- waste management and erasure
- security recordkeeping and review

Personnel Security

- personnel screening
- personnel controls

Physical Security

- barrier systems
- detection systems
- assessment systems
- access control systems
- physical layout
- security force
- warning systems

Environmental Controls

- air conditioning
- electric power
- water seepage and leakage

Disaster Control

- fire protection
- emergency procedures

Communications Security

emanations
encryption
terminal security
phone line security
communications alternatives

Computer Security

modern central processor
secure peripherals
militarized hardware
front-end machines
data base machine
modern operating system
secure subsystems
data base systems
password systems
security utilities
operating procedures
software development
software maintenance
batch input/output procedures
hardware maintenance procedures
communications procedures
periods processing

Once these controls are identified for each vulnerability which has been found, cost of these controls should be determined. These costs would include one-time costs of purchase and installaltion, the yearly cost of maintenance, organizational and personnel resources required, loss of productivity and other types of costs which can be anticipated. A cost-benefit analysis needs to be completed in order to evaluate how the safeguards can best be applied in a manner which neither leaves unprotected that which should be protected nor does not overspend on safeguards for losses which may be minimal.

Major Risk Analysis Approaches

There appear to be three major categories which sum up the state of the methodology. These are those which emphasize quantitative methods, applying formulae and statistical measures to discern both loss exposures and threat occurrence rates. A second category emphasizes more qualitative methods, attempting to more rank or structure those threats and losses which cannot be adequately or correctly expressed in numerical fashion. A third category combines these two approaches, using both the "hard" and the "soft" measures for various aspects to be measured.

Several of the most prominent approaches or those containing unique methodologies are: [Saltmarsh and Browne]

-Computer Resource Controls

-NBS/IBM Method (FIPS PUB 65)

-CITIBANK Method

-Jerry Fitzgerald and Associates Method

-Fuzzy-Metrics/SECURATE Method

-Relative-Impact Measure (RIM) Method

-Scalar Techniques

Churchman Ackoff Process

-Bayesian Decision Model

-Fault Tree Analysis

-Failure Mode Analysis

-Baseline Measures

Many of these methodologies may be more name than reality, since they may not be acceptable to organizational decision makers who seek easy answers to the hard security problems. In one case known to the author, a major bank decided that existing risk analysis models were too time consuming and toocumbersome and decreed that a risk analysis was to be completed in half a day. This meant that a Delphi session format was used as a means of reaching a consensus about threats, losses, and controls among security administrators, data custodians, data owners, data users, and auditors. Whether this is the wave of the future is not clear but it does appear that many of the more sophisticated risk analysis approaches will be considered as too difficult, too expensive, lacking valid data and/or too cumbersome for many organizations.

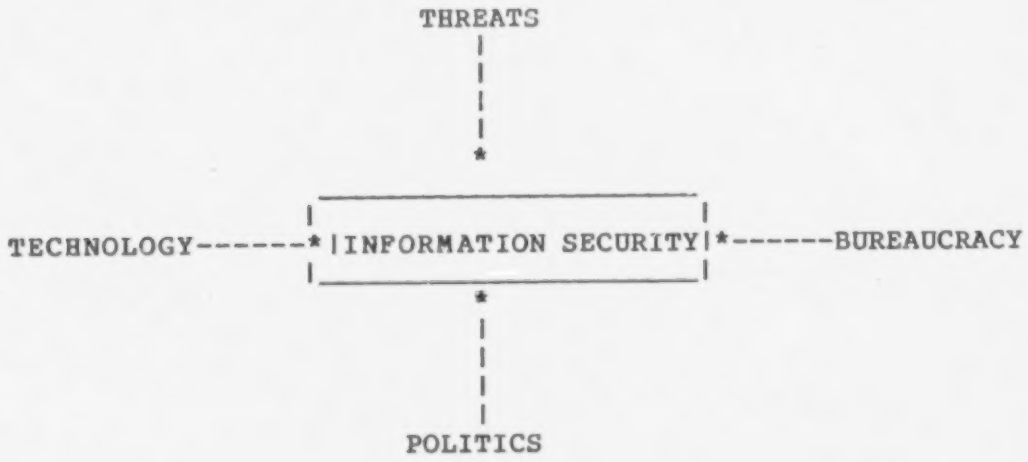
There does not appear to be a consensus at this time on whether risk analysis, with all of its difficulties and problems, can provide the type of assistance so needed to protect computer and telecommunications systems. The disatisfaction with risk analysis continues to be with its estimation procedures, which creates difficulties for those undertaking the analysis and for those who seek a more accurate and less "guestimate"-based process. The automating of risk analysis appears to simply take some of the drudgery away without providing better estimates. What alternative approaches might provide a better process for security of systems is not clear at this time and beyond the scope of this paper. Many of the general recommendations on how to improve the nature of risk analysis for scientific evaluations suggested by the Committee on Risk and Decision Making may well

be applicable to risk analysis for computer and telecommunications security. [National Research Council] How risk analysis will fit into the security and reliability efforts of the Federal Government is the topic of the next section.

IV. FEDERAL SECURITY AND RELIABILITY POLICIES

The need for Government information security derives from threats as well as technological, political, and bureaucratic forces. Technologically, the Government became aware of the great difficulties involved in developing appropriate and secure resource allocation and resource sharing during periods of rapid data and data processing growth. Politically, issues of privacy, protection of technological innovations, computer crime and abuse, and technology transfer to unfriendly nations played important roles in bringing the problem of information security to the agency levels. Bureaucratically, the development of information resource managers and processes, conflicts between national security and civilian Government agencies about definitions of information, and ongoing Congressional concerns over secrecy regulations contributed to information security becoming a politically charged topic.

FACTORS AFFECTING GOVERNMENT INFORMATION POLICY



Information security programs evolved from these pressures as well as from a series of directives and policies. While some of these statements were directly related to information security, others more indirectly addressed security. This mixture of sources has had an impact on how information security has developed. Particularly in the civilian agencies, information security efforts have suffered from a lack of basic definitions of what is information, how information can best be protected, and who will be in charge of such programs. As will be seen later in this paper, even the most current efforts in information security, the NSDD 145, contains concepts which may be contradictory and affect the potential for implementation.

A History of Federal Security and Reliability Policies

It is appropriate to start with a discussion of policies which affected information security while not having that as their major focus. In large measure, early information security efforts indirectly resulted from certain policies and this indirect means had implications for how later, more direct policies were developed. Much of the following is covered in much more detail in Becker. [Becker, TK 7885 E]

Four "indirect" legislative acts stand out in their impact on information security. The Brooks Act (P.L. 89-306), the Paperwork Reduction Act of 1980 (P.L. 96-511), the Crime Control Act of 1973 (P.L.93-83) and, the Privacy Act of 1974 (P. L. 93-597) all contributed to information security being placed within agency responsibilities. The Brooks Act is often considered as the impetus for the beginning of Government computer management.

The Act encourages the best management, use, and acquisition of automated data processing equipment and associated technologies. Specifically, the legislation requires that appropriate standards be developed to aid Federal agencies to effectively use information technology resources. Out of this, a number of computer standards and computer security standards were developed. The Paperwork Reduction Act was designed to encourage improved information policies and practices while strengthening Federal information-related activities. Specific provisions call for improvements through information resources management (IRM). The Act also contains provisions for the integration and coordination of Federal information policies, standards, and guidelines to be placed within OMB, requirements for effective use of ADP and telecommunications technologies, requirements for senior officials to be responsible for each agency's compliance with Federal policies, and an emphasis on data privacy, confidentiality, and protections against disclosures.

While both of these Acts emphasize effective management of Federal computer-related resources, two other Acts which had implications for information security emphasize confidentiality and privacy. Protection of citizens from Government and private sector intrusions into their lives became institutionalized with the passage of the Privacy Act and, to a lesser degree, legislation on crime control, education, and similar topics. The Privacy Act was designed to safeguard individual privacy by protection against misuse of Federal records and by requiring Federal agencies to adhere to prescribed controls to personal records dissemination and access. Federal agencies were required

to establish data protection rules and procedures and to provide safeguards to prevent misuse of information. The Act required OMB to develop rules and regulations to implement the Act and to provide continuing assistance for, and oversight of, the implementation of the Act by Federal agencies. The Crime Control Act, passed a year earlier, provides security and confidentiality of criminal justice record systems, requiring procedures to be established which would resonably insure that all information is adequately secured and privacy is provided.

Other Federal activities also affected the development of information security programs. The Foreign Corrupt Practices Act, while not explicitly mentioning computer security, has been interpreted as requiring the attention of top management in the private sector to put into place within their organizations adequate security measures, including those which could protect against misuses of computerized financial transactions. The President's Council on Integrity and Efficiency was established by Executive Order 12301. The Council was directed to focus on efforts to combat fraud and waste in Government, specifically by developing standards for the inspectors general in all agencies, efforts to develop a corps of auditors and investigators, joint agency projects and comprehensive plans for Governent-wide attacks on fraud and waste. Out of this has come a well documented study of computer crime in Federal programs and additional programs on responding to computer-related crime and abuse.

Each of these Federal actions and activities had an impact

on information security. Federal managers were being notified that information was a significant resource and that new standards and approaches were going to be required. More direct information on what was to be required developed from a series of policies, activities and reports which directly addressed information security and reliability. The major policies which directly addressed information security and created agency specific requirements came from the Office of Management and Budget. OMB has the overall responsiblity for guidance and policy on computer security. This is derived from statutory provisions and executive directives. The legislative framework for OMB's computer security responsibilities is from the Brooks Act, the Paperwork Reduction Act, the Privacy Act, and the Freedom of Information Act. The central policy statement regarding the responsibilities of agencies in security programs is OMB Circular A-71, Transmittal Memorandum No. 1, **Security of Federal Automated Information Systems**, issued July 27, 1978. A-71 specifies responsibilities for the development and implementation of Federal computer security by:

> defining the division of responsibilities among line operating agencies and central management agencies;
>
> establishes requirements for safeguarding personal, proprietary, and other sensitive automated data;
>
> defines controls to be incorporated into each agency's computer security program;
>
> establishes physical security policies, computer security procurements requirements, and personnel security policies.

The head of each agency is responsible for assuring the adequate level of security and the establishment of appropriate

safeguard requirements. Audits and evaluations are to be conducted and contingency planning is to be established and maintained. Certain security-related tasks are also given to the Department of Commerce, the General Services Administration, and the Office of Personnel Management.

OMB Circular A-123, **Internal Controls System**, prescribes polices and standards in establishing and maintaining internal controls. The nature of the controls required and the automated nature of many of the Federal accounting and administrative programs implies that computer security is central to control mechanisms. The Circular sets requirements for documentation, recording of transactions, execution of transactions, separation of duties, adequate supervision, access to resources, competent personnel, and reasonable assurance of security. In conjunction with OMB Circular A-108, **Responsibilities for the Maintenance of Records About Individuals by Federal Agencies**, security and integrity measures were made mandatory for Federal agencies. At present, OMB is revising A-71, partially due to the widespread criticism of the original memo as well as indications that its requirements are not being followed in Government agencies. Additionally, OMB is aware of the growth of telecommunication systems and changes in the nature of computer and information processing in the Government.

While much of the security emphasis in the policies described to this point have been applicable to computers, the other aspect of information security, telecommunications policy, was not adequately addressed. Partially, this was due to the nature of the information which was considered as requiring

protection by OMB and similar agencies. The emphasis was upon non-classified information held and/or processed by civilian agencies and concern was directed to processing issues. Insufficient attention was paid by those developing legislation and policy concerning telecommunications security. That security area was, however, being attended to by military and intelligence agencies which had become highly concerned with the vulnerabilities within their information processing system. From such concerns, a number of policies and directives requiring telecommunications security as well as computer security were established.

The Task Force on Computer Security issued a report entitled **Security Controls for Computer Systems.** The Ware Report, named for its chairman, focused on the U.S.'s increased dependency on computers and technological innovations which permit equipment and data resource sharing from different and geographically remote locations. The report attempted to protect computers and information in which users might share both the processing capability and the data. The Report presented " a security skeleton around which a specific computer system might be built." Key security principles presented included:

> adp systems shall accomodate, without exception, the responsibilities of individuals to ensure that certain official information affecting national defense is protected against unauthorized disclosure;
>
> a computer system shall grant access to classified information only to persons for whom it can determine that their official duties require such access, and thatthey have received the proper security clearances and need-to-know authorizations;

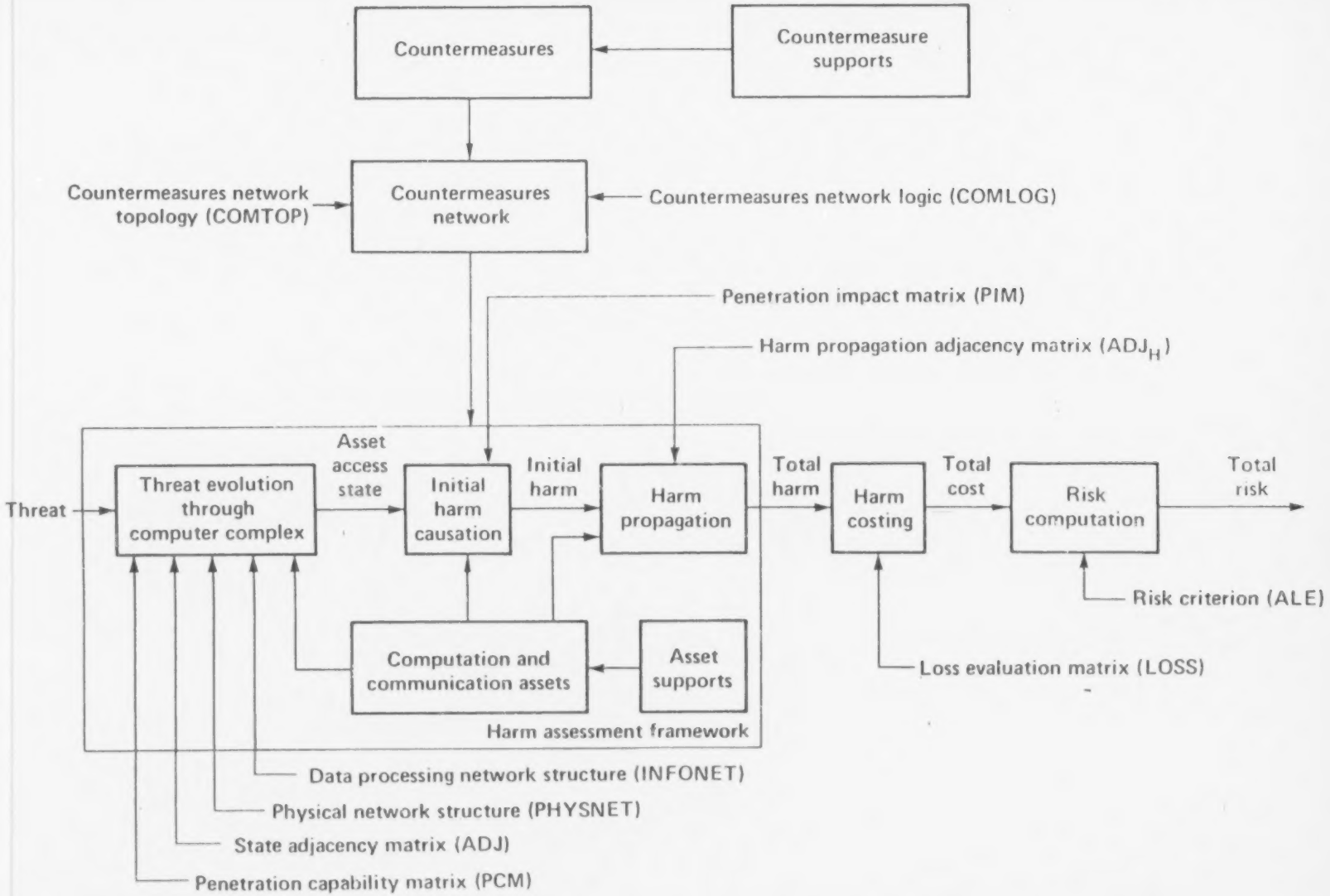
the means employed to achieve system security objectives shall be based on any combination of software, hardware, and procedural measures sufficient to assure suitable protection for all classification categories resident in the system;

to the maximum extent possible, the policies and procedures incorporated to achieve system security shall be unclassified. However, specific keys, passwords, authentication words, and specifically designated sensitive procedures shall require classification.

The Report provided a security system perspective to information security, emphasizing the requirements for the automation of a multilevel security system. Since then, a great number of other activities have been undertaken by the national security community in developing an effective approach to information security. One of the more publicly known undertakings was the work of the National Communications Security Committee (NCSC). **The National Communications Security Directive** of June 1979 designated the Secretary of Defense as the executive agent for communications security activities that protect Government-derived classified information and Government-derived unclassified information relating to national security. The NSCS undertook a review of the security policies of major Federal agencies. It was found that there were a variety of security perspectives and activities in these agencies, with the lack of central security authority and clearly established information security policy major obstacle to the protection of sensitive information. (Further information on the findings of the NSCS is found in a later section of this report.)

Related to the policy-making and structuring of agency security programs was activity on the part of the Government and the private sector to develop the Data Encryption Standard

(DES). This effort was made in recognition of the vulnerabilities of telecommunications systems and the needs to develop products which could be used for non-national security communications, both by civilian agencies and the private sector. The support for the development of the DES and the involvement of previously publicity-shy agencies (NSA) were symbolic of the importance of the DES, which served to change the nature of a previous Government monopoly over encryption devices and to extend the information security effort to agencies and organizations which had previously not been seriously affected by other security policies.



Risk assessment structure showing the essential elements of our assessment instrument and their relationship to the various stages of a risk assessment.

Source: C. C. Corynen, A Methodology for Assessing the Security Risks Associated with Computer Sites Springfield, VA.: NTIS, 1982.

An Overview of Stakeholders in Information Security

Information security came to be viewed as a problem due to certain key players, each of whom had a particular perspective on the problem. The players brought to the topic particular agendas, assumptions, and constituencies. These affected their involvements in supporting information security and their impact on its development. Five major players or institutions can be identified.

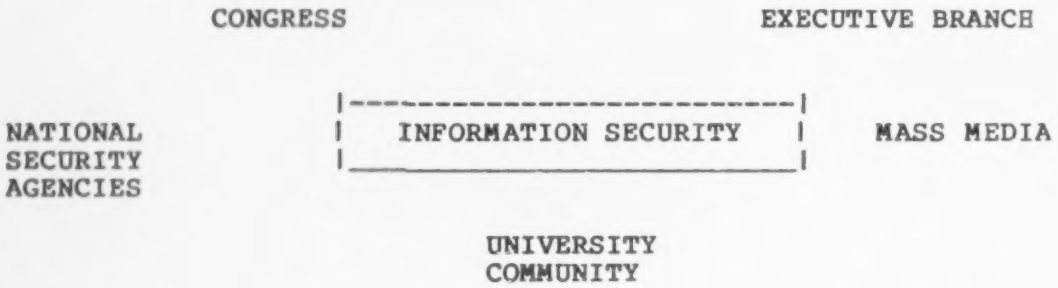
The first is the Congress, which became interested in information security through its concern with the management of Federal computer resources, computer crime and abuse, and Government secrecy and classification. The second major player is the Executive Branch, which produced a number of Executive Orders, Directives, and determinations on where information security responsibilities would be assigned. The third major player is the national security agencies, most specifically DoD, NSA, and certain of the services such as the Air Force. Their interest was in the classified information area but it became clear to them very early on that this was complicated by the resource sharing nature of their technology and the problems of multilevel data and users.

The fourth player is the university community, which became interested in information security due to their classified research projects and through the evolving of encryption as an academic topic. The universities, in that sense, were the recipient of security requirements from the national security agencies while also the site of academic research activities

which were worrisome to many in the national security agencies. Questions concerning academic freedom, censorship, and publish and perish reverberated between professors, agencies of the Government, and the Congress.

The last player is the mass media, which quite significantly defined the nature of the problem for many in the general public as well as for many of the other institutional players. The media helped to tie information security to such fundamental citizen issues as the rights of individuals to be protected from an intrusive Government, fraud and waste in Government programs, computer hackers, and computer crime.

STAKEHOLDERS IN INFORMATION SECURITY



The interests brought by these stakeholders were often quite contradictory, creating pressures and political battles which affected the nature of information security, both in the form of its policy as well as in its implementation. Complicating the problem even further was the complexity inherent within the dual nature of information security, the topic to be discussed in the next section of this paper.

V. THE DUAL NATURE OF INFORMATION SECURITY

Communications security and computer security are interdependent and, at times, seemingly indistinguishable approaches to information security. The boundary line between what is the computer system and what is the network is growing more difficult to specify and increasingly arbitrary. While computers and telecommunications have very different histories and traditions, their technological convergence means that they now share the same kind of logic, storage, switching, and transmission. Also, information handling systems now employ telecommunications and information-processing in such a way that it is difficult to say what is processing and what is communications. [Davies, et al.]

Similarly, there are growing pressures toward a merging of security approaches. However, communications security (COMSEC) and computer security (COMPUSEC), which are the two major approaches to protecting information, have significant technical and operational differences due to their separate histories, organizational structures, and technical perspectives.

The considerable differences between these two information approaches have important implications for how Government information security policies can be established and the potentials for full implementation. Additionally, computer security is a much more costly undertaking than is communications security. COMSEC measures were developed during a period when security was a major consideration and many of the developmental costs were spent years ago. Contemporary computer security measures are undergoing development and are evaluated not only

in terms of their security role but also in terms of how much they cost in comparison to what losses can or may occur. This requires computer security products to be reasonably priced in order to cost less that that which can be lost. It is no wonder that a NTIA listing of commercially available products for COMSEC listed some 160 products in 1980 while many fewer COMPUSEC products are just now being introduced.

The result of these major differences is that they have developed, and potentially will continue to develop, in a separate and uncoordinated fashion.

A Brief History of Communications Security in Government

COMSEC was a government monopoly from its early days and most clearly became established as such with the creation of NSA in 1952 and lasted until the 1970's. The Government was able to produce a wide variety of cryptographic equipment designed to protect everything from tactical voice communications to satellite telemetry.

This monopoly was challenged by a combination of events. Politics around the growing concerns of the citizenry about Government misuse of private data led to upwards of 200 bills pertaining to privacy to be introduced during the 93rd Congress alone. [Becker, Issue Brief Number IB 74105, 21 March 1975] Technology changed as well with the advent of integrated circuit technology bringing high grade cryptography within the practical reach of a much broader set of potential users. Added to that, expert mathematicians, computer scientists and engineers from

universities and corporations outside of Government became interested in cryptology and soon were producing extensive information. The market was no longer limited, well understood and controlled, the essential features of the Government monopoly. One of the most public testimonies to this challenge to the monopoly was the controvery around the Data Encryption Standard (DES). The suspicions around the Government's continuing threat to personal privacy and the growing knowledge of these outside experts who were willing to challenge Government actions and claims resulted in a public controversy over the design and security of the DES. The controversy became so bitter and raised so many questions that the Senate Select Committee on Intelligence found it appropriate to formally investigate the involvement of NSA in the development and possible weakening of the DES so that the DES would be secure enough to protect Goverment codes but vulnerable enough so that NSA could break it. The Committee's conclusion that NSA had not tampered with the design of the algorithm hardly seemed to put to rest the controversy. In 1976, the concept of the public key cryptography was presented by Diffie and Hellman. This was an alternative to the DES, since the enciphering key would be publicly available while the deciphering key would not be, thus alleviating some aspects of the problem of key management. During this period of time, there was rapid computerization of businesses. These businesses were also interested in protecting data, from possible industrial spying as well as to meet the requirements of the Privacy Act, Fair Credit Reporting Act, and other legislative

requirements. This created an economic motivation for the development of cryptographic devices. The Government's monopoly had been challenged and appeared to have been broken. With the stakes high, the Government decided to shift its policy and to attempt to establish cryptography once again as a major (and potentially controlled) Government concern. Encryption information became a national security topic.

On November 16, 1977, Presidential Directive/NSC-24 was signed. It called for improved telecommunications protections for government-derived, unclassified information which may be of value to a foreign adversary. PD-24 is extremely important, for not only did it officially acknowledge for the first time that even some unclassified information required protection but it assigned responsibility for the protection of some U.S. governnment communications to an agency outside of the military and intelligence communities. Unclassified Government information which might be useful to an adversary was to be protected and non-Government information useful to an adversary was to be identified and the private sector informed of the problem and encouraged to take appropriate measures.

Responsibility for protective measures designed for the security of classified information and other information related to national security was to be the responsibility of the Secretary of Defense. This followed previous policies. The Secretary of Commerce was given responsibility for Government-derived unclassified information and the enhancement of communications protection and privacy for the commercial and private sectors. Communications security had been split up, with

the civilian agencies and private sector under non-military leadership. In essence, the protection ofGovernmentrelated communications became a divided responsibility between the DoD and Commerce. Problems in defining ownership of data and security responsibilities, which were difficult to define in an environment where communication lines and links carried a variety of types of information, fell on a newly established agency, the National Telecommunications and Information Administration (NTIA).

NTIA had several major problems to face in accomplishing its responsibilities. One problem was that of NSA, which was much more powerful and with a long history of involvement with communication security problems. How was NTIA to work independent from NSA or join with NSA in a joint strategy while keeping its independence? Another problem was that of distinguishing betwen information related to national security and that which was not. Some of the difficulties involved in such an effort would be how to protect individual items of information which by themselves have no security significance but in combination do as well as the problem of how to protect links which contain both national security significance and non-national security significant information. While PD-24 specified protection from foreign threats against non-national security information, the protection of privacy of individual

communications also was covered by the Directive. NTIA appeared to concentrate on the foreign threats issue alone, leading to GAO to report that

> ...since NTIA has not considered electronic transmission containing personal data useful to (foreign) adversaries, it has no ongoing effort to develop guidelines for protecting personal data in the telecommunications environment." [GAO, LCD-81-1, November 12, 1980]

NTIA's battle to control one aspect of communications security was completely lost once it was viewed as unwilling to recognize the legitimate role of NSA in communications security. With the advent of the Reagan Administration, NTIA underwent rapid decline in budget and influence. The "two authorities" approach to communications security had been halted, considered by many in power as a failure. A single authority was increasingly being viewed as necessary for protecting what had become an even more complex computer/telecommunications environment.

A Brief History of Computer Security in Government

Computer security has a much shorter history than communications security. 1967 serves as a starting point, for during that year the CIA recognized computer security as a unique security discipline when it appointed a Special Assistant for Automatic Data Processing within the Office of the Director of Security and within the DoD, computer security was raised as an issue through the Industrial Security Program.

Early studies concentrated on the area of multilevel secure operating systems. The first operating system designed to be

consistent with a specified security policy model, the 1967 ADEPT 50 system, enforced many aspects of DoD policy. Under the Air Force Electronic Systems Divsision (ESD) and DARPA, a number of analytical studies, formal security models and theories, and security operating system prototypes were developed. [Committee on Multilevel Data Management Security] A task force was formed under the chairmanship of Willis Ware of the Rand Corporation. The task force was directed to study and recommend appropriate computer security safeguards that would protect classified information in multi-access, resource-sharing systems. Out of this report, **Security Controls for Computer Systems**, DoD formed an ADP Security Task Force to develop policies, culminating in DoD Directive 5200-28, **Security Requirements for Automatic Data Processing Systems**, and **DoD ADP Security Manual 5200.28M**.

Reinforcing the need for policies and procedures were tests on the vulnerability of computer systems to penetrations. Military "tiger team" efforts to penetrate commercial systems were so successful that no commercially available systems of that day withstood their efforts and no existing system was considered adequate to enforce required security for classified information. Even those systems which had special security added to correct known implementation errors and design oversights were found by the tiger teams to be penetrable. After a series of studies to support the design and verification of multilevel security systems, a panel was tasked with preparing a development plan for a coherent approach to attacking the problems of multilevel computer security. The Anderson panel recommended starting with

an ideal system and to create design mechanisms that implement that model system. Out of that came the idea of the security kernel, control mechanisms over access of subjects to objects within a system. After much work by MITRE, SRI, Honeywell and System Development Corporation, processes were developed for system design specifications. Great efforts were undertaken to move this research along despite shifts in emphases and in funding sources within the Government. In June of 1978, the Computer Security Initiative was officially launched. This was formed to foster the development of "trusted systems" through technology transfer efforts and to define reasonable ADP system evlaution procedures to be applied to both government and commercially developed trusted ADP systems. [**Proceedings of the Seminar on the DoD Computer Security Initiative Program**] In 1982, this long history of efforts and bureaucratic waring finally led to an agreement that NSA would establish a new computer security center to be called the DoD Computer Security Center, which was to serve the Department of Defense.

On the civilian side, the Institute for Computer Sciences and Technology (ICST) has provided public and private sectors with practical guidance on how to secure computer-based information. The program encompassed research and development of security standards, technology transfer to potential implementors and vendors, and assistance to users of security technology. It has been involved in the issuing of the Data Encryption Standard (DES) and has also been active in security standards for personal computer security, risk analysis, EFT message authentication, personal identification, contingency planning, and computer

security certification. Among its other activities are the sponsorship of numerous workshops and symposia, presentations at conferences, and publication of reports and the Federal Information Processing Standards (FIPS) series.

VI. The Present State of Government Information Security

The present state of Government information security has been described as a muddle. There is no single organization with overall responsibility for information security, responsibility is divided along civil-national security lines while computer and telecommunications systems act in an integrated fashion to process varieties of information. The impact of this muddle is potentially quite serious.

> Because today's federal policy concerning cryptography is oriented almost exclusively to current narrowly defined national security concerns, there has been limited consideration of why federal support of independent private-sector competence in cryptography may be necessary and desirable within the coming decade.
>
> Today's policy structure, based on an adversary relationship, assumes that national security interests and independent nonmilitary interest in cryptography are necessarily in significant conflict. However, the national security, more broadly defined, may be increasingly threatened by the growing vulnerability of civilian electronics and information systems. [Victor C. Walling, Jr. et al.]

Some attempts have been made to recognize the problems involved in these separations of responsibilities and often antagonistic relationships between agencies which are responsible for aspects of information security. One major effort was undertaken by the National Communications Security Committee

(NCSC) which is the group responsible for COMSEC policy. In January, 1980, a Computer Security Working Group was appointed to examine those aspects of computer security that relate to teleprocessing systems and to develop objectives, policies, and implementation procedures for consideration by the NCSC. This Group called for a national level group to review the problem and to recommend a "national level approach" to information system security policy. In order to avoid previous problems, the Group suggested that participation by both the national security and non-national security communities be assured to recognize the requirement to protect all types of sensitive information. They also stated that there is a need to develop policy to deal with data in telecommunications sytems and computer networks where the needs for systems security in the future appears to be greatest. The Group notes some of the problems from the past by stating that

> ...the amount and nature of existing computer security policies on one hand, and the results of various...oversight activities on the other, suggest that the root problems of computer security program implementation in the field are not going to be substantially ameliorated by simple promulgation of additional overall policy.
>
> Moreover, the comprehensive nature and recency of the promulgated OMB computer security policy requirements suggest that issuance of aditional overall computer security policy per se from a different and potentially competing 'national' level source may, in fact, be counterproductive. [National Communications Security Committee] The report warns against a new policy effort leading to further confusion on the part of agencies, a duplication of effort, conflicting guidance, dissipation of already scarce resources and expertise, and even possible government embarrassment.

There is a separate but related effort underway stemming from the DoD Security Program of the Computer Security Technical

Consortium. This was established to provide:

> coordination of the DoD research and development efforts in computer security
>
> a focus for technical aspects of certification and implementation of multilevel security systems
>
> technical leadership for the transfer of the state-of-the-art computer technology.

A major focus of the Program is to promote the development of "trusted computer systems" which have sufficient integrity so that they may be used in shared environments in which data security classifications vary. Specific program activities undertaken have included a series of DoD/NBS technical seminars on computer security. These have involved other Government agencies and the private sector in discusssions on common areas of concern. Another activity is the DoD-wide computer security evaluation center program management office. On October 25, 1982, DoD Directive 5215.1 established the Computer Security Evaluation Center (CSEC), which would have responsibilities for the technical evaluation of trusted systems. Under the Directive, an Evaluated Products List (EPL) and a Consolidated Computer Security Program (CCSP) were also established. Other efforts were being taken by the Office of the Assistant Secretary of Defense (Comptroller), where the IRM Sysems Directorate had implemented an approach to good management practices consistent with DoD directives and OMB's A-71. These included policy guidance on security and life cycle management, training of computer security managers by the DoD Computer Institute, and other coordination efforts.

In addition, information security efforts have been taking

place under the TEMPEST program, which is a component of the National Communications Security Committee, although managed by NSA. Begun in the mid-1950's, it evaluates and screens companies and equipment to assure that compromising emanations or electromagnetic radiation from computers and other information technologies are eliminated or controlled. TEMPEST approved equipment and systems are placed on the Preferred Products List of the Special Committee on Compromising Emanations. A final program worth briefly mentioning is the DoD Industrial Security Program. This Program is directed to safeguarding classified information within industries which require access to classified information. This Program has an ongoing effort to achieve industrial security efforts at appropriate levels and to set forth policies, practices and procedures to assist other Government agencies and the private sector to meet necessary levels of security.

The multiple efforts to meet the challenges of information security have created a hodgepodge. There continues to be an abysmally low level of attention paid to the problem and protections put in place to prevent misuse, abuse, and theft. Both the NCSC effort to define appropriate policy on the national security side and the efforts of OMB operating on the civilian side have enunciated the problems with existing policies but have been less successful in determining what information policy can and should be supported. "The assessment, then, of the current status of computer security is that the culprits are riding in automobiles while the cops are still on horseback." [Fordyce]

National Security Decision Directive 145.

NSDD 145,**National Policy on Telecommunications and Automated Information Systems Security**, dated September 17, 1984, is a basic guidance document for the U.S. in the Information Age. The NSDD, attached to this report as an appendix, is based upon an appreciation of the importance of the technical merging of computer and telecommunications systems. This merging, made possible by technical advancements, creates greatly improved efficiency and effectiveness while also posing significant security problems for Government as well as the private sector. The Directive establishes mechanisms for the merging of communications security and computer security, two hitherto separate disciplines and approaches. The security definitions of information and lead agency responsibities for ensuring adequate security have been placed in military and intelligence agencies, potentially leading to what could be considered as extraordinary power in peacetime over the classification and treatment of information in civilian Federal agencies.

A Summary of NSDD 145

NSDD 145 provides objectives, policies, and an organizational structure to guide national activities in safeguarding systems which process or communicate sensitive information. It is a government-wide directive initially focusing on those automated information systems which are connected to telecommunications transmission systems. Special recognition is given in the Directive to requirements for protecting intelligence sources and methods.

Major objectives of the Directive are:

a. a reliable and continuing capability to assess threats and vulnerabilities and to implement appropriate, effective countermeasures.

b. a superior technical base within the Government to achieve this security, and support for a superior technical base within the private sector in areas which complement and enhance government capabilities.

c. a more effective application of government resources and encouragement of private sector security initiatives.

d. support and enhancement of other policy objectives for national telecommunications and automated information systems.

Information requiring degrees of security are (a) Government classified information which will require security by such means as are necessary to prevent compromise or exploitation, (b) sensitive, but unclassified information, whether Government or Government-derived, the loss of which could adversely affect the national security interest, which will require protection in proportion to the threat of exploitation and the associated potential damage to the national security, (c) private sector information falling into either of the categories above.

The Systems Security Steering Group will be established as a senior level group to oversee the Directive and ensure its implementation. The Group will be chaired by the Assistant to the President for National Security Affairs. The National Telecommunications and Information Systems Security Committee will be established under the Steering Group as an interagency group at the operating level. It will consider technical matters and develop operating policies as necessary to implement the

Directive. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) will chair the Group. The Executive agent of the Government for Telecommunications and Information Systems Security will be the Secretary of Defense while the National Manager for Telecommunications Security and Automated Information Systems Security will be the Director of the National Security Agency.

Some of the most significant activities authorized under this Directive have to do with definitions of information and the potential impact of these definitions on civilian agencies. NSA will examine "government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation...(and) review and assess annually the telecommunications systems security programs and budgets of the departments and agencies of the Government, and recommend alternatives, where appropriate for the Executive Agent and the Steering Group" (Section 7, paragraphs a and j) Additionally, the Director of OMB shall specify data to be provided during the annual budget review by the departments and agencies of programs and budgets relating to telecommunications and automated information systems security and provide such data after consolidation to the National Manager via the Executive Agent. OMB is also to amend as appropriate OMB Circular A-71 (Transmittal Memorandum No. 1) and OMB Circular A-76, as amended, to make these policies and regulations consistent with the Directive. (Section 9, paragraphs b1-b3)

Analysis of NSDD 145

NSDD 145 is built upon earlier Government efforts, often failed efforts, to define appropriate types of information requiring security, determine how to handle the different needs of civilian as well as national security agencies, and combine COMSEC and COMPUSEC. Whether the Directive can overcome these earlier problems is partially dependent upon how it develops during its planning phases.

While the end of the Directive states that the examination of the facilities of departments and agencies requires the approval of the head of the department or agency, the clear implications of other sections of the Directive as well as the nature of Government operations may well result in the exceptional involvement of military and intelligence agencies within civilian agencies. Civilian agencies may find that other agencies operating under this Directive are in position to establish classification over data, require certain security mechanisms, and review the appropriateness of budget requests for security controls. Each of these issues needs further discussion.

The Directive covers classified information as well as other sensitive but unclassified information, whether Government or Government-derived, the loss of which could adversely affect the national security interest. However, information, per se, is not the major objective of the Directive. Rather, systems which generate, store, process, transfer, communicate, or handle such information are the focus for security. As noted in the second

introductory paragraph of the Directive, classified national security information and other sensitive information concerning the vital interests of the United States "...even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate." "Even if unclassified" suggests that information of all types, even if not classifiable on their face, may be classified as a precaution.

The Directive is absolutely correct when it points out the capabilities of information processing and intelligence gathering techniques for combining disparate information into new forms of data. The correctness of the insight concerning the technology does not, however, suggest how certain established balances between agencies and sectors of the U.S. Government should best be formulated. The implications of the Directive's point concerning the possibilities of the combination of unclassified information into a new form which can have security implications is not clear in terms of how information policies should be determined nor who should be in charge of such an effort. Efforts have been made within the Federal Government to have the program persons and the IRM directors be the persons with major information definition and control responsibilities. The potential of this Directive is to remove one important aspect of that responsibilitity and to centralize the definition of

information security within other agencies of Government, possibly within NSA, according to a close interpretation of the Directive.

A second major implication of the Directive is that agencies operating under the structure of NSDD 145 may be put in the position of being reviewed and required to follow certain security policies and procedures not defined within their environment nor of their own creation. Some of this potential is inherent within the capability to define information security levels. Further, however, the Directive seeks to set certain security standards legally applicable to Federal Departments and Agencies (Section 9). The National Manager (Director of NSA) will also review for the Executive Agent and the Steering Group the aggregated automated information systems security program and budget recommendations of the departments and agencies of the U.S. Government and recommend alternatives, where appropriate. The National Manager also will examine Government telecommunications systems and automated information systems and "...evaluate their vulnerability to hostile interception and exploitation...(and)...prescribe the minimum standards, methods, and procedures for protecting cryptographic and other sensitive technical security material, techniques, and information." (Section 7, paragraph i)

The third issue which has policy implications regards controls over costs. OMB is required under the Directive, to review OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the Directive's subject matter. A-71 has

been considered as a civilian-oriented policy statement whereby OMB carries out its mandated position. Current thinking in OMB regarding their revision of A-71 is to emphasize that program directors are the key personnel to determine and be held responsible for information security. If those persons are accountable, they are not only the agents in charge of defining the security levels of information within that agency but also responsible for proposing and cost justifying security aspects for budget reviews. OMB has in fact traditionally taken the position that security must be built within budgets as appropriate items rather than presented as separate line items. This approach to information security would appear to be undermined by the NSDD, since information definitions and security requirements would be defined by other agencies, most likely NSA and DoD. This would mean that OMB's model would require program managers to request security funding as determined by other agencies of the Government. Agency and departmental security costs would come out of their own budgets without their having sufficient control over fundamental definitions or considerations of cost-justification . OMB may have to decide whether it wishes information to be defined centrally or not, for that determination will affect how A-71 can be structured, how responsiblity can be designated within agencies, and what reviews will be appropriate for agreeing to security costs for agencies.

A last important policy consideration is the proposed relationship between the Government and the private sector.

While there have been cooperative security efforts between these two sectors in a number of areas (Tempest, DES, industrial security, technology tranfer), it is evident that this Directive seeks to expand this into aspects of information security which have not been controlled except during emergency periods in our national history. The Directive is intended to "...foster an appropriate partnership between government and the private sector in attaining these goals (to promote a coherent and coordinated defense against the hostile intelligence threat to systems)." (Introduction) A major objective of the Directive is to develop support for a superior technical base within the private sector in areas which complement and enhance government capabilities and a more effective application of government resources and encouragement of private sector security intiatives.

> "The government shall encourage, advise, and where appropriate, assist the private sector to: identify systems which handle sensitive non-government information, the loss of which could adversely affect the national security; determine the threat to, and vulnerability of, these systems; and formulate strategies and measures for providing protection in proportion to the threat of exploitation and the associated potential damage....In cases where implementation of security measures to non-govermental systems would be in the national security interest, the private sector shall be encouraged, advised, and where appropriate, assisted in undertaking the application of such measures." (3c)

The Systems Security Group is required to identify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and to recommend steps to protect such information and to identify systems which handle sensitive, non-Government information, the loss and exploitation of which could adversely affect the national security interest. Federal Information Processing

Standards for the security of information in automated information systems and Federal Telecommunications Standards for the security of information in telecommunciations systems will be issued for public use. Such standards, while legally applicable only to Federal Departments and Agencies "...shall be structured to facilitate their adoption as voluntary American National Standards as a means of encouraging their use by the private sector."(9a) Such a promulgation has been considered as inappropriate by such groups as the IEEE Technical Committee on Security and Privacy. Given earlier discussion of the broad nature of the definition of potentially damaging information and specific mention that Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation, a potential for major changes in government relationships with the private sector may be under way. Since government or government-derived information is explicitly mentioned and information, even if unclassified in isolation, often can reveal highly classified information when taken in aggregate, this Directive may serve to redefine information security within the private sector, whether or not Government information is directly used or whether specific threats and vulnerabilities can be determined. It would appear that the Directive seeks to involve the private sector by the setting of minimal standards as well as by raising the possibility of national security-related information being misused by hostile forces. Additionally, the Directive may be authorizing growing Government contributions or other inducements

for private sector research and development of information security products. This may be the resolution of the policy issues concerning how the government might best create the necessary security tools and mechanisms.

NSDD 145 is an outgrowth of many earlier attempts on the part of the Government to respond to the issues of information security. It is not clear from the Directive or from reports about earlier meetings of agency representatives how the Government will resolve those nagging problems which have plagued earlier efforts. Potentially the most important, and possibly the most controversial ingredient in this latest effort is that NSA will be taking on a much more important role, both with its relationship with civilian agencies of Government as well as moving from its leadership role in communications security to a broader role which also encompasses computer security. The implications of this is not yet clear but potentially it will be an area of deep concern for the Congress.

VII. PROBLEM ISSUES IN INFORMATION SECURITY

From our discussion to this point, there may appear to be a great amount of Federal attention being paid to information security . Unfortunately, it appears that there may be more effort but less impact, during a period when purchases in technology are growing, computer-communications links are expanding, and the amount of potential loss to centralized data and resources is estimated to be enormous. This section of the report will contain a discussion of major problem issues relating to the review of Government security and reliability efforts.

OBSTACLES TO INFORMATION SECURITY IMPLEMENTATION

It is evident that there have been significant obstacles to implementing information security. The GAO and various Congressional committees, have produced a large number of reports over the years on this particular problem. These reports provide information on the types of obstacles which have been found with information security and serve on a more general level to indicate the problems which may occur with newer efforts, such as the revision of A-71 or NSDD 145.

There are several general problem areas which have been cited, the first of which has to do with the lack of central leadership to provide a "...clear and well defined set of national goals protecting computer and communications systems. (This) continues to be a serious limitation in establishing an effective national program." [**Computer and Communications Security and Privacy**, p. 28] Presidential Directive 24, which outlined Federal communications security, has been criticized for

failing to clearly pinpoint the distinct responsibilities of the National Security Agency and the Department of Commerce in carrying out the security program. This lack of strong national leadership was mentioned by a leading expert who had developed one of the earliest security research and policy reports. Dr. Willis Ware stated:

> No entity in government has addressed the general policy issue of what constitutes a comprehensive top-to-bottom prescription for installing security controls, nor identified the many dimensions of such policy and made it avialable as guidance. It is being done piecemeal; every agency is inventing it for itself or not doing it. [Ibid.,p. 29]

A second problem area has to do with the lack of clear security requirements. OMB, the agency responsible for certain aspects of this leadership, has been charged with having failed in this regard. For example, the GAO reported that A-71, the OMB policy statement did not:

> identify the minimum controls necessary for ensuring a reasonable level of protection over personal, proprietary, and other sensitive information
>
> clarify the relationship between Transmittal Memorandum No. 1 and policy and guidance on safeguarding information classified for purposes of national security
>
> clarify when executive agencies must afford the same level of protection against unauthorized disclosure of personal, proprietary and other sensitive information as they do to information classified for purposes of national security
>
> establish policy and specific guidance for achieving a reasonable level of protection over those systems using telecommunications networks

A third problem area is that agencies have failed to treat information security as a serious problem and there has been limited support by senior management. Many agencies were found to have a lack of basic controls, failed to pinpoint

responsiblities, and did not undertake even limited compliance with statutory or regulatory requirements. There have been limited allocation of resources for computer security, a lack of comprehensive security programs, security functions not being placed at sufficiently high levels, nor sufficient independence form operational functions. One GAO study found:

> limited resources committed to and used for risk management
>
> failure to define data processing operations in accordance with OPM criteria for personnel security programs
>
> failure to provide reliable contingency and backup hardware and software
>
> failure to provide an appropriate separation of duties between information security officers and data processing managers.

A fourth problem area is the difficulties related to implementing information security, particularly in civilian agencies. Some of the problems cited against OMB are in reality problems inherent in information security. Among these are the lack of a workable definition of what is a reasonable level of protection for Federal information systems. The complications of developing such a definition is suggested in the criticism that OMB did not translate the broad social goals of the Privacy Act of 1974 and openness in Government concepts of the Freedom of Information Act into the design and implementation of policies

and systems. The Deputy Director of OMB, Joseph Wright, stated in testimony that the problems of security have indeed grown worse since the A-71 was formulated.

> Things are changing dramatically...The rapid growth and reliance on information technology really brings to the front the need for an effective Federal computer security program. We don't have enough coverage in areas like microcomputers. We also don't have enough coverage of the areas of telecommunications. These areas were not a major focus during the mid-1970's. [Ibid, p. 30]

These four problem areas are indicative of the serious complications involved in developing an information security program for the Government. These will be raised in terms of certain basic policy questions in the last section of this report.

BALANCING PREVENTION AND PRODUCTION AS COMPETITIVE REQUIREMENTS

A major consideration for the Government's heavy investment in information processing is that it increases production in labor intensive environments. Security is quite often viewed as contrary to or an interference with this effort toward more productive Government operations.

Production and prevention are, in fact, competitive requirements in an office setting. While they need not be, certain security efforts suffer from certain stereotypes, often conjuring up images of guards, locks and alarms. These tasks are considered as the more appropriate responsibility of security personnel who come from law enforcement backgrounds, rather than employees involved in "more productive" work. Further, many nontechnical users and managers may well assume that security is

built-in or somehow automated so they don't need to be responsible for it. Many, if not most users, tend to have limited appreciation of how computers can be misused for crime and are unwilling to take on security responsibilities since they do not consider it their own work responsiblity. Even if these problems could be overcome, they may not even know how to become more security conscious.

Many of the computerized operations are exactly those operations which have traditionally had the greatest amount of white collar crime. Computerizing those operations has often been accompanied by cutbacks in certain supervisory or auditing personnel. As a result, many computer operations are minimally controlled or supervised. The kinds of unauthorized acts that can be accomplished with computers present new problems of control. To combat these problems, computer security requires effective managerial controls. Unfortunately, many of the controls found in organizations today are traditional approaches that evolved before the computer era began. An indication of this is found in the following exhibit [Adapted from Campbell]:

TRADITIONAL CONTROL PROCEDURES AND COMPUTER PROCEDURES

Traditional Control Procedures	Computer Procedures
Never allow the same person to create, authorize, and enter a transaction	Automate data at their source, creating, authorizing, and entering a transaction as one step
Make certain that accounts in one department agree with totals maintained in another department	Create loosely structured , transaction-driven data-based systems that permit update of data base from multiple entry points
Segregate check authorization from check writing and require two signatures of authorized signers on each check	Use preprinted forms with automated check-signing machines to sign checks authorized for issue by the computer

In an environment where there is rapid computerization and limited abilities to involve end users in the roles that they can and should play in information security, the potential for managers to have to make a choice between production and prevention are much too real. While the production questions are those which have to be faced daily, and for which a manager may well be evaluated, prevention or security issues are less immediate and more easily put off until there is an absolute need or until it is too late.

Further, information security officers are in a unique position, for they are critical to the success of any security effort while they are also in a quite unclear and "insecure" role. As the bearer of bad news, they may identify a problem or a possible flaw and then face the risk of: [Becker,TK 7885 E]

being ignored

not having the problem advanced to the appropriate decision level

being given too few resources

being requested to suppress or limit an investigation

being moved to another assignment

Information security officers thus have to learn how to protect their jobs as well as to protect Government assets and resources.

The problems of obstacles to information security implementation and balancing prevention and production as competitive requirements are highly important for the continuity and security of this society. The problems which have been mentioned in this section of the report will continue to be an important area of concern in the near future. The nature of computerization and the growth of computer crime and abuse appear to be a technological byproduct. How much more serious the problem can grow and the possible responses available to the Federal Government are the topics to be covered in the next section of this report.

COMPUTER CRIME

VIII. COMPUTER CRIME LEGISLATION

Computer crime legislation is a topic of great public interest as well as of national importance. While there has been a great amount of discussion and public furor, the legislative efforts made to date, on the state as well as the Federal levels, are not encouraging. The speed of technological advancements and of the growth of computer crime may well have outpaced the legal responses of the Government. There continue to be major ambiguities in the law concerning how to respond to computer crime and problems in achieving basic definitions and understandings about crime causality. Certain assumptions and working priorities have become embedded within proposed crime legislation, leading to symbolic stances, unrealistic penalties, and the creation of potentially unprosecutable law.

Factors Affecting the Development of Computer Crime Law

There are serious questions about the nature, extent, and direction of computer crime. Yet, little of this uncertainty or lack of definitive conceptualization is found in proposed computer crime legislation. Much of the legislative effort to date has been based upon relatively simple-minded assumptions about computer crime and computer criminals. The lack of an established knowledge base and the mass media-influenced push for legislation have created the potential for an ineffective response to the problem.

There are a number of relatively simple-minded general assumptions affecting how computer crime legislation is

developing. A first assumption has to do with crime causality. Assumptions treated as certainties have affected legislative approaches to such issues as the types of individuals committing these crimes, their reasons for such acts, and the punishments considered as appropriate or necessary. For example, if teenage hackers are considered as the major culprits, their objectives in committing such acts to challenge the technology, and the damage that is done mainly the invasion of files, then legislative goals would be directed to that problem.

In fact, in testimony given before Congressional committees and in public statements of legislators, hackers tend quite often to be considered as the prime computer criminals. Legislative efforts on regulating computer crime often have significant hacker-type sections, overlooking the fact that a quite large proportion of cases of computer crime have been committed by trusted inside employees who have minimal computer sophistication. Much of this emphasis on hackers and other forms of computer crime stems from the role of the media in affecting public opinion as well as legislative interest. The lack of sufficient empirical research on computer crime combined with the media definitions of crime have created pressures for quick legislative responses rather than laws which can be based upon years of legislative and legal precedents.

A second assumption underlying the legislation is that computers and telecommunications are only somewhat different from other forms of technology. Much of the current criminal and business law is based on earlier forms of technology and is quite often lagging behind technological developments. Just as law

required fundamental reformulations upon the creation of the Industrial Revolution, so the law may require such reformulation during the Information Revolution. One who has argued the usefulness of existing law has been Roy Freed, who, in a non-computer crime context, states that it is impossible to stop applying existing rules to manifestations of computer technology while a new body of law is formulated since there are legal questions being raised now. An effort to devise a new body of law would entail the identical activity that should be performed in undertaking to apply existing rules and this exercise would produce no different results if performed properly. He states that

> ...the rules of law actually are dynamic and responsive to social needs when new fact situations are described accurately from a legal point of view. Complaints of the inadequacy of existing rules with respect to computer subject matter mask frequently either desires for legal treatments that are incompatible with social policy, such as the enlargement of rights of copyright owners, or failures to perform the legal steps professionally. [Freed]

The legislative response to catching up with computer technology has been limited. A few states have passed computer crime legislation simply by redefining property to include intangible forms. This treats computer and telecommunications as only slightly different from other forms of technology. Essential considerations on the nature of trespass, forms of evidence, determining factors for establishing damages, and even more difficult issues of definitions of property may have to be considered in order for computer crime legislation to be adequate and appropriate for legal purposes. Similarly, considerations

may have to be given to how much emphasis should be placed on civil versus criminal law and on patent and copyright laws in the computer age.

This uncertainty about the technology is also seen in the lack of a consistent definition of computers, telecommunications, and related terms found in the legislation proposed on the state and Federal levels. There appears to be no clearly established definition or little agreement on how to define the technologies. Legislative definitions range from narrow to broad conceptualizations. One of the most common definitions of computers is Colorado's, which reads:

> an electronic device which performs logic, arithemetic or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network.

Among the simplest of the definitions is Connecticut's, which defines computers as "a programable electronic device capable of accepting and processing data." Among the more complex of the definitions is that of Virginia, which defines computers as:

> an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term `computer' includes any connected or directly related device, equipment or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.

Related to the need to define the technology is the need to redefine certain existing statutes. Joseph Wright of OMB commented that:

> (A) review of applicable telecommunications security legislation showed that the Communications Act of 1934 and the Crime Control Act of 1968 are inadequate with respect to interceptions of wire communications, or `wiretapping.' The 1934 Communications Act did not define the term `interception.' The Crime Control Act of 1968, as amended, used the qualifying term `aural acquisition' (acquired by ear) to define interception. As a result, only interceptions by aural means are illegal under this act, unless authorized by court order. Therefore, we conclude that as long as the term `aural' remains as a semantic qualifier in the 1968 Crime Control Act definition of interception anyone can conduct unathorized nonaural wiretapping of data telecommunications without a court order and not be in violation of this law.[U. S. Congress. House Committee on Science and Technology]

A third and final assumption, in reality more of controversy, affecting how computer crime legislation is developing is whether computer crime is a new form of crime or not. If computer crime simply is traditional types of crime with the computer being used as the crime tool, then traditional types of laws may be quite applicable and major new legislation may not be necessary. The issue may hinge upon the question of whether there is anything distinctively different about computer crime. This obviously is related to the earlier types of assumptions discussed. The answer to the newness or originality of computer crime, which is partially an empirical question, may affect what laws may need to be created as well as determinations on what agencies, on the state and Federal levels, will lead the fight against computer crime.

Federal Laws Applicable to Computer Crime

If computer crime is not a uniquely new crime, then existing law may be quite applicable. [**Computer Crime: Legislative Resource Manual**] According to one expert, a Federal prosecutor would be able to charge and seek conviction for a Federal computer crime under one of the nearly forty potentially applicable federal statutes. [**Hearings on S. 240**] Another expert [Nycum] has divided Federal statues applicable to computer crime into seven broad categories:

-theft and related crimes
-abuse of Federal channels of communication
-national security offenses
-trespass and burglary
-deceptive practices
-malicious mischief and related offenses
-miscellaneous other statutes

None of these statutes were designed originally to control computer crime, causing prosecutors to "shoe-horn" cases into applicable law. Such an approach has substantial procedural and substantive difficulties. [Glynn] The most frequently applied statutes are the Federal wire fraud statute, the Federal mail fraud statute, the transportation of stolen property statute, and the theft and related offenses statute. Analysis of case law tends to indicate that the absence of a precise statute to combat computer crime can create difficulties in gathering and presenting computer-generated evidence and jeopardize the prosecution of criminal activity involving such sophisticated technology. If the court fails to construe the statute liberally, there will be instances where cases will be lost. As a result of this difficulty with using existing law for

prosecution, there have been calls for specific computer crime legislation drafted to sufficiently define the wrongful activity, deter future computer crime, add certainty and uniformity to these prosecutions, and encourage reporting of such crimes. [Wharton]

The passage of computer crime legislation on the state as well as the Federal levels has not meant, however, that some of the more problematic aspects of computer crime have been adequately addressed. Several of the major problems with existing legislation include:

(a) unclear definitions of basic concepts, such as trespass, intent, damages and appropriate punishment

(b) lack of impetus for organizations to respond to computer crimes, including requirements for prevention, detection, and reporting mechanisms to notify authorities.

(c) clarification of the need for a simple trespass violation to respond to unathorized access acts.

(d) lack of consistency of terms and approaches concerning computer crime from state to state.

(e) determinations of jurisdiction over cases which involve interstate intrusion or other cross-jurisidictional cases. [Nycum and Appleman]

Thus, legislation to regulate computer crime is a complex problem which must address complex issues. In the following section, the history of Federal computer crime legislation is discussed, leading up to a discussion of currrent legislation.

History of Federal Computer Crime Legislative Efforts

Since the 95th Congress, the Congress has considered various measures to protect computers and other systems. [For a thorough review of Federal computer crime activities, cf. Becker, TK 7885

E, February 3, 1983] Much of the early concern was with problems associated with Federal computer related resources, as reflected in the landmark studies from the Senate Committee on Government Operations (now the Committee on Governmental Affairs), **Problems Associated with Computer Technology in Federal Programs and Private Industry** and **Computer Security in Federal Programs.** The Chairman of the Committee, Senator Abraham Ribicoff, was a key person in creating interest in the findings and in sponsoring the first Federal bill on the subject, the Federal Computer Systems Protection Act of 1977, S. 1776. The lack of action on the bill led Senator Ribicoff, along with his previous co-sponsor, Senator Charles Percy, to introduce a similar bill in the 96th Congress, the Federal Computer Systems Protection Act of 1979, S. 240 with an identical House bill also introduced in each of these two sessions, first by Representative Rose and then by Representative Nelson. Once again, no further action was taken after hearings were held. In the 97th congress, Representative Nelson introduced H.R. 3790 which was similar to the earlier computer crime bills. No action was received on this bill either.

Since that time, a large number of legislators have become involved in the topic. For one, Rep. Dan Glickman held hearings on computer and communications security and privacy as the chairman of the House Subcommittee on Transporation, Aviation and

Materials. His report, released this year, contained a number of important recommendations which went beyond legislation, including:

> Congress should charter a national commission to examine the vast set of interrelated issues surrounding the security and privacy of computer communications systems and have the commission outline a framework for policy and guidance of future Federal Government actions.
>
> The Administration should begin an immediate assessment of the problems and issues in order to develop a set of national policies that will ensure the protection of relevant critical national systems relevant to Government, industry, commerce, and the society.
>
> Existing resources within the computer security community (vendors, computer security experts) and the Federal Government should be channeled to pursue expanded reserach efforts to improve computer/communications security.
>
> The Administration should strengthen clearance procedures for Federal workers handling sensitive non-national security data.
>
> The private sector should be encouraged to develop a certification process and a voluntary standards program to give users information on the specific capability of a device or technique as well as to indicate the condition or environment that permits optimum functioning.
>
> Training should not be limited to technical personnel but should also include managers, users, and operators so that all personnel associated with information systems will understand their role in protecting computers, communication networks, and data.
>
> OMB should consider the advantages of establishing a non-national security data classification scheme to protect certain categories of sensitive data in the Federal Government.
>
> The Administration should develop uniform standards for identifying and reporting computer crimes and abuses.

As can be seen, these represent a merging of earlier information security concerns of the Government with computer crime legislative issues. Representative Glickman has indicated that he will be following up these recommendations with hearings and other reviews of Government activities in the future.

Criticisms of Past Computer Crime Legislation

Senator Laxalt, who has been instrumental in the Administration's bill on computer crime entered in August of this year and who will play an important role in upcoming computer crme legislative efforts, expressed what he considered as the four major areas which required attention and examination. These are:

> 1. To what extent would S.240 (or any other bill) contribute to Federal jurisdiction into areas trditionally reserved to the states?
>
> 2. What is the evil to be remedied? What is the incidence of computer crime and what are the costs to our society?
>
> 3. By focusing on the computer as an instrumentality, are wc exposing individuals to criminality for possibly innocent conduct while not at the same time furthering the public safety?
>
> 4. Does S.240 (or any other bill) properly define the context in which a computer may be viewed as a possible instrumentality of criminal acts? Has Congress properly understood the intricacies and dimensions of a very complex question? [Senate Committee on the Judiciary. Subcommittee on Criminal Justice]

These questions appear to sum up what has continued to be essential difficulties in addressing adequate and appropriate computer crime legislation.

Certain additional reservations have been stated during hearings and in comments made by public officials. One concerns the breadth of the bills, with some witnesses expressing concern that the bills might expand Federal jurisdiction to include many private sector computer systems since these systems use a communications carrier involved in interstate commerce. Others have raised questions concerning the definition of computers found within the bills, suggesting that too broad a definition would allow an attempted repair of a pocket calculator to be considered as a crime. Witnesses have raised questions on the possible effects the law might have on new applications of technology, such as electronic funds transfer, with some suggesting that these special applications might require more specific statutory controls. Some were concerned that Federal criminal jurisdiction would be expanded by these bills. Senator Hatch, for example, expressed concerns that S. 240 in the 96th Congress was not needed since there were over "forty sections of the United States Code, provisions of the Electronic Funds Transfer Act, provisions of the Financial Institutions Act, and provisions of the Privacy Act, that have direct utility to Federal prosecution of computer abuse. [Ibid] Senator Laxalt stated that S. 240 expanded Federal criminal jurisdiction into areas not previously covered, especially those reserved to the States. [Ibid] A consistent criticism has been the lack of adequate evidence and information on the scope of the computer crime problem and solid information on the success of such legislation in prosecuting computer criminals. Few of these questions or criticisms have been adequately met in past

legislation and present efforts toward creating this specialized law may not resolve these issues.

Current Legislation as of the End of the 98th Session

As of the end of the 98th Session, there existed several pieces of computer crime legislation on the Federal level and a variety of laws on the State Level. The Small Business Computer Security and Education Act of 1984 is an effort to provide information and training through the SBA to small businesses to protect them from computer crime problems. The major computer crime bill, however, was passed as part of the anti-crime amendments to the stopgap budget bill just before the Congress adjourned in October. The bill that passed was Representative Hughes' H.R. 5616, with two sections (1030a1 and 1030a4) deleted. The bill prohibits unauthored access to a computer to obtain classified information that protects national security, the unauthorized access of a computer to obtain financial information that is protected from disclosure by the Right to Financial Privacy Act and the Fair Credit Reporting Act, and unauthorized access of a computer owned by or operated for the Federal Government when the perpetrator knowingly uses, modifies, destroys or discloses information in that computer. This last provision has been heavily criticised by the ACLU as an open invitation to prosecute "whistle blowers" rather than computer abusers. While a case using the legislation has been brought in Florida, it appears that this computer crime law is quite limited, for example, in not covering the private sector, and

does not seem to satisfy the various interest groups which are seeking a fuller law. The next session of the Congress may well hold several major hearings and other actions related to computer crime legislation, including efforts by Senator Laxalt on the recently passed bill and Senator Leahy on improving privacy by closing gaps in Federal wiretapping laws.

The states have been quite active with legislation and there are now some two thirds of the states which have some form of legislation. The variety of state laws is an indication that there does not appear to be a consensus of what are the basic problems of computer crime or the most appropriate legal responses. Some of the states have emphasized the hacker problem, others the issues of privacy, while others have acted to simply get some law on the books. Some new areas have developed in states, with Massachusetts, for example, providing a very broad definition of technology in its proposed legislation and Connecticut, as another example, stressing privacy considerations more than other states. The "local politics" of a state, i.e., political interests, types of industries, and local leadership will increasingly be applicable to how computer crime legislation will be defined. There is no evidence that state efforts are affecting Federal considerations except for the fact that one of the nation's first computer crime bills (in Florida) was sponsored by Bill Nelson, who subsequently became a Congressman where he has continued his efforts for legislation on the Federal level. It is not clear at this time how the Federal-state division of labor will be decided, with determinations made on where computer crime enforcement efforts are most appropriately

and most easily accomplished. It may be that the LEAA experience , where Federal funds, models, and other supports were offered to the states and local law enforcement officials, will be considered as the most appropriate future model. On the other hand, Federal developments in information processing, secrecy regulations, interstate commerce decisions, growth of national data bases, banking trends, and mandating of computer security efforts may well portend an overwhelming Federal role in computer crime prevention on the state level and in the private sector.

The Administration's Proposed Legislation

The Administration's computer crime bill, The Federal Computer Systems Protection Act of 1984, was presented in August of 1984. This was a legislative proposal to establish Federal criminal penalties for offenses involving computers. At the time of the presentation of the bill, there were no discrete Federal statutes tailored to deal with computer crime, although the Hughes bill was making its way through the Congress. As a result of the lack of a computer crime bill, prosecution of computer-related offenses was difficult. The bill is important, not only because it represents an area of high legislative concern to the Administration but because its form and focus may serve as a model for subsequent legislation on the state as well as the Federal levels.

The bill would make it a Federal felony offense to engage in computer-related fraud or theft or to damage or destroy a computer, computer program, or information stored in a computer.

These felony sanctions would apply to offenses involving computers owned or operated by the Federal Government or a Federally insured financial institution, or other computers where the offense involves two or more computers operating in different states or in a state and a foreign country. The bill would also establish Federal misdemeanor sanctions for unauthorized access to a computer owned or operated by the Federal Government or a Federally insured financial institution.

The bill would amend Title 18 of the U. S. Code. Section two of the bill adds a new section (1028) to Title 18, proscribing computer fraud and other crimes involving computers. The proposed section is drafted in language that is taken from the mail fraud (18 USC 1341) and wire fraud (18 USC 1343) statutes to the maximum extent possible. This emphasis upon the fraud statutes is a central point in the Administration's approach. Rather than emphasizing computer crime, per se, there is an emphasis upon the misuse of a vehicle (mail and/or wire) rather than an emphasis upon the medium through which the misuse was conducted (the computer). According to various persons who were involved with the drafting of the bill, this is a "prosecutor's bill" in that it provides Federal prosecutors with clearly defined understandings of what activities are to be considered illegal and offers the necessary ingredients for the preparation of a successful case. As stated in the bill, "it is intended that the extensive body of law that has been developed interpeting these (wire and mail fraud) statutes apply to the new subsection (being proposed)." This means that approximately one hundred years of history involving fraud can be used by judges

in making their decisions on cases involving computer and telecommunications-related crimes. Questions of a person's knowledge of whether the act was illegal or not, decisions on a person's intent in committing an act, and other potentially difficult evidentiary issues can be dealt with by statutory intepretations which emphasize fraud related to the consequences of an individual's actions.

The bill appears to have other aspects which are responsive to criticisms made against earlier state and Federal proposals. The first is that of Federal versus state jurisdiction and decisions on who will gain predominance over computer crime cases. The Administration's bill only covers three types of computer systems. These are computers owned by, under contract to, or for or on behalf of (a) the U.S. Government, (b) certain financial institution, and (c) other computers where the offense involves computers located in two or more states or in a state and a foreign country. There appears to have been careful thought given to this third category so that the language would respect state and local jurisdiction over purely intrastate offenses, with the Federal role limited to instances where the Federal Government could make a unique contribution. In the third category, the contribution may be due to the nationwide reach of Federal legal processes, such as subpoena power to cross state lines, investigatory agencies which have specialized

resources, and expertise beyond those readily available at other levels of Government.

The second aspect of the bill which appears to be responsive to earlier criticisms is the issue of damages. The Administration has taken an approach to property which emphasizes property, including intangible and intellectual property, as having a market value in the world. That provides a factor for determining damages. Potential punishments will be $20,000 or imprisonment for not more than one year, or both and, under another subsection, no more than $50,000 or imprisonment not more than five years, or both. Additionally, forfeiture to the U.S. of any interest acquired or maintained in any computer and computer software which has been used to commit the violation will be possible as the court shall deem proper upon conviction. This latter aspect relates to the need for some means of gaining court involvement in recognizing how a crime has affected a victim, whether an individual or an organization, and allowing victim impact concerns to potentially lead to double damages and forfeiture.

A third related issue found in the bill is the definition of fraud, computers, and property. The definition of defrauder given in the bill is:

> Whoever having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by false or fraudulent pretenses, representations, or promises, or to embezzle, steal, or convert to his use or the use of another, property not his own, for the purpose of executing such scheme or artifice or embezzlement, theft or conversion or attempting to do so, knowingly accesses or attempts to access a computer

Computers and computer networks are defined as:

> an electronic, magnetic, electrochemical, or other high speed data processing device performing logical, artihmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device...computer network means two or more interconnected computers, computer terminals or computer systems

Property is defined as:

> including, but not limited to financial instruments, information, including electronically processed or produced data, and computer program and computer software in either machine or human readable form, computer services and any other tangible or intangible item of value

It is too early to measure the applicability of the bill or its potential for passage. Few Federal agencies appear to have analyzed the bill and, possibly due to the lateness of its introduction, there has been relatively little Congressional discussion. The only criticisms of the bill which have surfaced are that it contains definitions of computers and abuses which are extremely broad and it lacks any provisions stating that a minimum level of financial gain must be derived from a trangression to be considered as a felony.

VIX. A DEVELOPMENTAL MODEL OF FUTURE COMPUTER CRIME

This section contains information on how certain crimes develop from activities performed by individuals into group-supported enterprises. This "natural history of crime" will provide insight into how certain new forms of crime become invented and the process by which they become organized into large scale activities with group structured motivations, opportunities for crime, and services to support criminal acts. The purpose of this exercise is to draw upon sociological and criminological insights into the organization of crime and to suggest how this pattern of development might be applicable to predicting future computer crime patterns.

In general, there are four major theoretical approaches to crime causation. [Sykes] These are that crime tends to be caused by (a) the structure of society which limits legitimate means to achieve acceptable societal goals but provides illegitimate means toward those goals, (b) the disorganization or ineffectiveness of formal as well as informal agencies of social control, (c) crime is learned as part of a normal learning process in associating with people who hold criminal values or atitudes, and, (d) certain behaviors and individuals become labeled as deviant and this categorization creates self-fulfilling prophecies of criminal acts.

These approaches tend to agree that group supports are an important aspect of crime, particularly in socializing individuals into criminal acts and thinking patterns. Studies of prostitution, drug abuse and sale, burglary, and other criminal behaviors have established the importance of group supports for

learning how to commit criminal acts and how to establish new views of self and of the world. A central element in this group support is that it increases the novice's motivations, opportunities, and means of committing crimes. While criminal acts are possible without group supports, group supported and sponsored crimes are easier to commit, more predictable in terms of what to expect, and more rewarded within a group culture.

In order to deviate, there are a series of factors which are required and which can most easily be obtained from criminal groups. These factors include skills on how to commit crimes, supplies of needed tools and skills, social support from new peers, symbolic support for a new set of behaviors different from previous acts of an individual, and even the means of neutralizing moral messages from the world at large about one's activities. That is, crime is an organized activity, where one needs to locate sources for learning technical criminal skills and perceptual skills required for successful predictions as to where the greatest benefits might be located. [Letkemann, Sutherland, Jackson, Best and Luckenbill, Schur]

Applying these thoughts on a different theoretical level, it is possible to suggest that some criminal behaviors become more advanced and, from a societal viewpoint, more troublesome, when they become group supported. As a crime moves from an initial stage where it is "underdeveloped" to more specialization and sophistication, there are stages that the crime, and individuals associated with that activity tend to go through. This can be viewed in terms of the stages of crime growth, similar in general

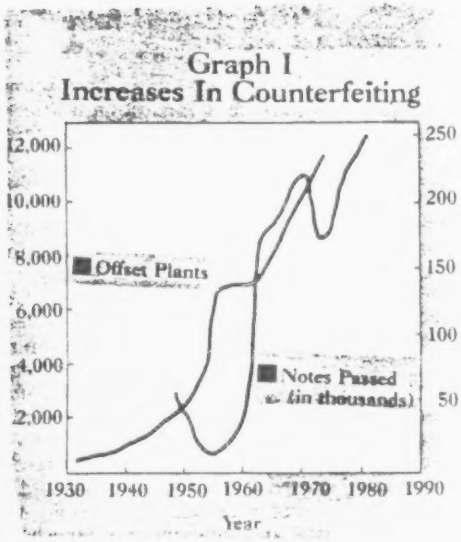
ways to the four stages of EDP growth. [Gibson and Nolan] The stages are (1) Initiation, (2) Expansion, (3) Formalization, and (4) Maturity.

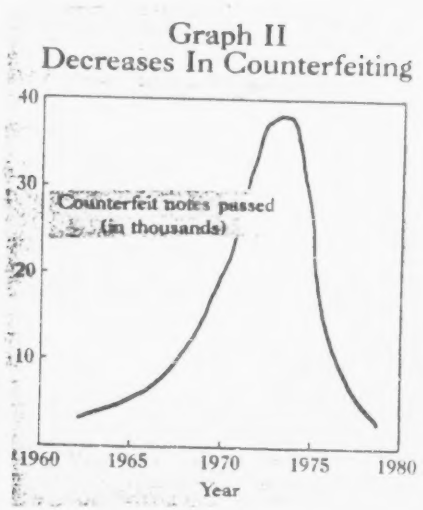
Initiation is the starting point for certain crimes, when they are developed, found, first tried, or in some other fashion introduced. Individuals are trying out these new methods and trying to determine how successful they might be. Hit and miss techniques are attempted and ideas are traded between individuals. The expansion stage occurs when there are enough individuals with skills, opportunities for crime, and/or sufficient rewards for a growth in the number of these new crimes to occur. This is a stage where individual criminals are testing the limits to their new techniques and attempting to determine whether this crime is worth pursuing. More and more individuals are becoming interested in this particular crime and there are those who are awaiting the determinations of the expert criminals before they join in on such activities.

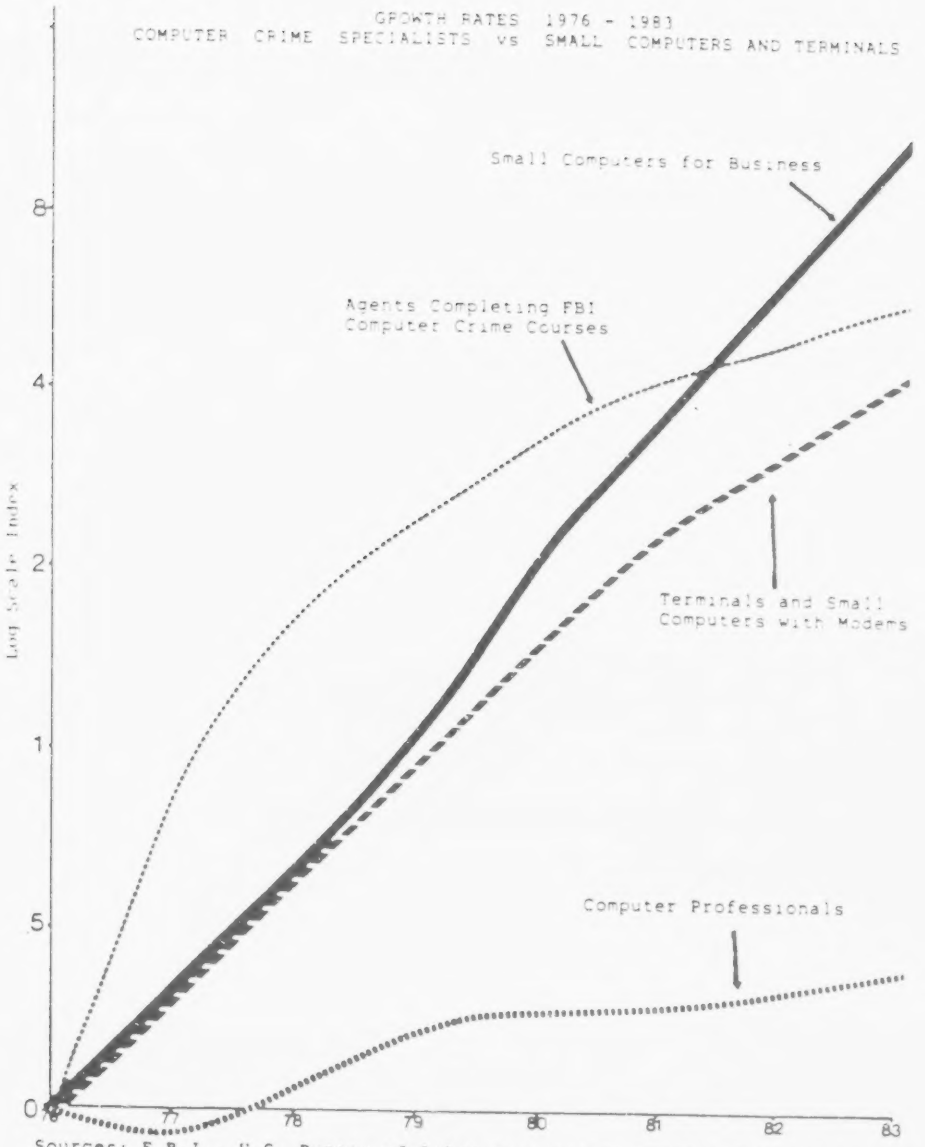
The formalization stage is the period when individuals start to specialize in certain aspects of that crime and working patterns are becoming established. During this period, law enforcement officials have become aware of a growth in certain new types of crimes and are attempting to understand the pattern. Depending upon how serious, visible, or problematic the crime is considered, they attempt to determine how best to marshall their limited resources. Law enforcement responses to the crime become a consideration in how the crime develops during this formulation stage. Group efforts are directed to determining opportunities for crime and certain services required for the commission of the

crime are obtained. The group develops the means for creating the crime and determining the best means of making the crime successful, such as creating ways of selling the stolen goods, determining where bribes might be required, learning new technologies which have been created to protect products, and deciding when and how crimes are best committed. The final stage is that of maturity, where the rules are clearly established and the expertise has been developed. Here there are group supported and directed efforts which structure who will commit what crimes and under which conditions. In some instances, there may actually be a monopoly formed, where only certain people are allowed to commit certain crimes. The probabilities of success as well as arrest and conviction are able to be somewhat accurately estimated, based upon previous experiences with the crimes, victims, law enforcement, and public interest in the crime. The crime has become institutionalized, until technology, the law, and/or criminals change the nature of the crime pattern which has been established.

An example of how a particular crime can grow, at least in the number of incidences, is illustrated in the following graphs. The first graph compares the growth of offset plants and notes passed, illustrating the tenfold increase in counterfeiting that occurred after the introduction of improved offset plants, which was a new technology. Graph II shows the trend line for counterfeit notes, illustrating the decrease in counterfeiting which followed the introduction of a new deterrent, color ink, to the currency in several countries during the mid-1970's. [Batelle


Graph I
Increases In Counterfeiting
12,000
10,000
8,000
6,000
4,000
2,000
250
200
150
100
50
Offset Plants
Notes Passed
(in thousands)
1930
1940
1950
1960
1970
1980
1990
Year


Graph II
Decreases In Counterfeiting
40
30
20
10
Counterfeit notes passed
(in thousands)
1960
1965
1970
1975
1980
Year



Sources: F.B.I., U.S. Bureau of Labor Statistics, Frost & Sullivan, I.R.D.

(International Networks)

Factors Affecting Future Computer Crime Developments

The technical milieu of today's society is undergoing changes which could contribute to increased opportunities for certain types of crimes, in particular, forms of computer crime. At the same time, the methods by which computer crimes are committed are undergoing a "maturation" process, with indications that there are significant shifts in how crimes are being learned and how they are being committed. All of these factors can have an impact on how individuals can calculate the risks and opportunities for such crimes, potentially creating new ingredients in their motivations to commit computer crime. The end result may be a whole new type of computer criminal in the future, who has new structures for evaluating opportunities for crime and new techniques for successful committing these acts.

These comments require further specification. There are a number of factors which will influence whether and how computer crime will develop in the future. The technical changes which could contribute to increased opportunities for computer crime are, at the same time, some of the most powerful and beneficial aspects of technical developments. Increased ownership of computers, a growing computer literacy in the population, further miniaturization of equipment, increased remote access, and expansion of multiprocessing capabilities are some of the technical potentials we have learned to expect in the Information Age. Yet, the underside of these advancements is that they can serve not only authorized processing but also unauthorized processing. This is illustrated in the following chart. [Sherizen]

TECHNICAL DEVELOPMENTS AND POSSIBLE COMPUTER CRIMES

Technical Development	Possible Crime Activity
High speed and complex processing	Bypassing poor password controls without detection, allowing access to funds disbursement operations.
Large number of users with equipment, knowledge, and potential access capabilities	Misuse of agency computer equipment to gain access to sensitive files.
Decentralized systems with multiple users, a variety of equipment, and multiple access points via communications lines	Unauthorized dial-up access to classified data.
Concentration of data in data base management systems	Employees gaining access to data as part of their work, allowing potential for data manipulation.
Certain technical employees have on-line capabilities to design, develop, and/or operate systems.	System modifications which could bypass security system controls, allowing sabotage or check generating capabilities.

This table specifies a number of the capabilities of computers and supplies the possible crimes which could be committed using that capability. If we add to that chart the other technical develops which are being introduced daily, it is evident that there are many ways by which friendly user features can be very friendly with the wrong users.

Modes of Learning About Computer Crime

Computer crime methods currently appear to be undergoing changes at this time and most likely will continue in the future, although the pattern of the development is impossible to predict.

At this time, there are certain ingredients in the development. While difficult to quantify, at least some of the computer crimes found to date were the result of "copy cat crimes" which followed the methods of others. There was a diffusion of information from an individual or group of individuals who determined a way of penetrating a system to other individuals and groups. Some of this diffusion was through the showing of Wargames and the media coverage of the 414's in Milwaukee. These hacker exploits served to attract attention to what was quite possible to do and provided lessons on how to do it. It may be possible to forecast the level or type of spreading of computer crimes by predictive epidemiology, much as this has been used for predicting terrorist activities. [Kupperman]

There are a number of sources for learning about computer crime. Even before the hacker exploits, there were specialist magazines and clubs as well as electronic bulletin boards across the nation. For example, there is at least one publication publicly available through the mails on how to steal from automatic teller machines, and it has been reported that over 1000 copies have been sold and it is in its third printing. Several national hacker newsletters are also readily available. Passwords, codes, telephone numbers, techniques, and technical

insights are presented in articles and on some of these bulletin boards. Among the sorts of information which can be obtained are the following which have been found on certain electronic bulletin boards: [Maxfield]

> lists of customer billing codes and common carrier access numbers
>
> access numbers, passwords, and logon procedures for mainframe computer systems
>
> procedures for wiretapping and phone bugging
>
> lists of phone numbers of famous people, government installations, computer systems, and telephone operator call routing codes
>
> Programs for downloading to convert a home computer into a blue box or to use for scanning for modem numbers of customer billing codes
>
> lists of credit card numbers to be used to order merchandise over the phone for resale or trade.

Many of these boards are open to anyone to use, although some of the more elite ones or those which are operated by persons worried about being investigated, have instituted quite sophisticated access controls. One expert has stated that he has had more difficulties in accessing these special boards than in gaining entry into some high security Government systems.

Professionalization of Criminals

This is not to suggest that the hackers are the only threat or that they are the only ones who are interested in learning about how to penetrate systems. Studies by Parker and others have suggested that inside employee are more of a threat to most organizations than the outsider. In some cases, those employees who are undergoing training in information processing or who in

some other fashion have access to equipment may be those who have knowledge and willingness to steal. Tentative findings from the President's Commission on Integrity and Efficiency support this reasoning, where it has been found that the lack of basic personnel screenings and supervision contributed to certain employees committing crimes.

In one sense, many of those who have been caught committing computer crimes have been amateurs rather than professional criminals. While some of them have been quite sophisticated in the ways of crime, others were found due to their lack of knowing relatively simple procedures to cover their tracks or to limit the signs of their activities. Professional criminals, on the other hand, may have a much more sophisticated set of skills which they have brought or can bring to computer crime. Once professional criminals and/or organized crime becomes involved, then the stakes become much higher and the problem potentially much more serious. It has been stated that organized crime has been approaching various hackers to try to get them to work together. One can imagine what the consequences might be if the hackers were working with organized crime to tamper with banking and credit data computers. [Maxfield] Articles have appeared indicating that some crime is becoming computerized, including a nationwide gambling ring which maintained a central mainframe computer tied to microcomputers in 43 branch offices, a computerized data base with an inventory of automobile parts stripped from cars stolen from across the country, and a prostitution ring used a centralized computer system to track its workers. [Computerworld, July 23, 1984] It is quite possible

that criminals are purchasing the latest in computer security products, both to reverse engineer them to learn how to bypass their protections in order to gain entry to victim's systems as well as to better protect their own systems.

Evolution of Specialized Criminal Skills

While predicting new techniques for computer crime is quite difficult, it is clear that there will be increases in opportunities for computer crime (with the growth of equipment and centralization of data), more means available (with the development of new techniques of computer crime and the establishment of information exchange of these techniques), and more potential criminals (as computer knowledge increases and as more people use computers as part of their work). The growth of micros linked to mainframes suggests that this will be a major problem area. Users, whether authorized or unauthorized, may be in position to access live mainframe data, select what they want and manipulate the data in real time. When the quite limited protections in place within Government and private sector systems are considered, the rapid increase in the number of knowledgeable individuals with their own micros and modems is potentially a very serious problem.

Many of the computer crimes now identified will become modified or bypassed as security controls become established. Penetrations through password guessing will become more difficult as the access control mechanisms become strengthened and structured. However, new techniques to penetrate through insecure operating systems will be attempted. There may well be

an increase in collusion, with insiders who have knowledge of vulnerabilities and loopholes in systems and outsiders who may have technical knowledge of systems. As large corporations and major Government agencies become more security minded and increase their preventions, there may be an increase in new targets, in a form of displacement of crime. As persons who had never committed a crime before realize how easily crime can be committed, there may be increased number of attempts in organizations which have not been victimized previously. There is also the potential for some extremely high losses to occur from computer crime as people find out how easily crime can be committed. Finally, there will most likely be an increase in the "schools for computer crime," electronic bulletin boards and other means of finding out new techniques and new opportunities for crime.

Public Response to Computer Crime

An important aspect of how computer crime will develop in the future is the public perception about computer crime and computer criminals. This public perception will have an impact on computer crime in two major ways--determining whether computer crime is defined as a serious problem and influencing how Government actions and computer crime law will develop. If computer crime continues not to be viewed as a serious issue or, somewhat as at present, a form of teenaged acting out, then this can serve to reinforce or to create a message of acceptance of this type of activity. This may, in fact, be viewed as a legitimization by those who are considering committing a computer

crime. In the same way, the lack of public uproar about computer crime and the limited ways that the public understands the problem suggests that there will be few constituencies pushing for computer crime legislation. Ironically, the passage of quite limited computer crime law may meet the needs of the public for something to be done about computer crime and undercut legislative and enforcement efforts on the part of the authorities to seriously respond to the problem.

The question of how seriously the public will treat computer crime will depend, to a degree, on how they understand their stake in the problem and who they view as the victims of computer crime. A Roper poll found that 39% were very concerned about reports of embezzlements and rip-offs through the use of a computer while a total of 74% were very concerned about crime in general. [Dutton and Meadow] This fits with other surveys taken on white collar crime which indicate little knowledge or interest in the more complex and potentially less directly threatening problem. The first cases prosecuted under computer crime legislation will be highly important in influencing public opinion. Depending upon who is being charged, what type of criminal act is committed, who the victim is, and the public's general perspective on punishment at that time, a consensus may well be formed about computer crime which can have a lasting impact on how future cases will be treated. It is quite possible that the public's interest in computer crime but its lack of appreciation with its seriousness can provide a very mixed message to lawmakers who are interested in responding to public

opinion. The message may be that something should be done about the problem but what that response might be is quite unclear.

Computer Crime Cost-Benefit Considerations

A final factor which will affect how computer crime will develop in the future has to do with the motivations and perceptions of potential criminals. The crime cost-benefit analysis which can provide an individual with the potential rewards and losses of a crime will be influenced by all of the factors given above. For example, the strength of computer crime law and the vigor of legal authorities in pursuing computer criminals will be one consideration while the opportunities for committing crimes and the availability of applicable crime methods will also be factored into some individuals' decisions to commit crime.

In addition, certain types of computer crimes may be considered more attractive, depending upon the types of victims or victim organizations involved. Crimes against certain unpopular organizations are often viewed less serious or simply as repayment for previous arrogance by that organization.[Smigel] In Government, certain agencies tend to be less popular with the public and may serve as appropriate targets for certain persons. Examples include the IRS, Social Security, EPA and the various law enforcement, defense, and intelligence agencies. The discussions in the mass media about how much computer crime is occurring and how great the losses are could serve to whet the appetite of certain individuals, creating a false sense of opportunities to get away with vast amounts of money with minimal chances of being caught. All of these factors will be entered into a "computer crime risk analysis," to determine whether someone will think that the chances of getting caught are greater than the gains to be received.

FACTORS AFFECTING THE FUTURE GROWTH OF COMPUTER CRIME

MODES OF LEARNING ABOUT COMPUTER CRIME

PROFESIONALIZATION OF COMPUTER CRIMINALS

EVOLUTION OF SPECIALIZED CRIMINAL SKILLS

PUBLIC RESPONSES TO COMPUTER CRIME

COMPUTER CRIME COST-BENEFIT CONSIDERATIONS

COMPUTER CRIME LEGISLATION AND LEGAL ACTIONS

X. PROBLEM ISSUES IN RESPONDING TO COMPUTER CRIME

This section of the report has contained information on the problems involved in establishing computer crime legislation. In addition to the legislative difficulties, there are technological and social trends which also appear to increase the potential growth of computer crime now and in the near future. This perspective on computer crime suggests that neither a "technological fix" nor a "legislative fix" will supply sufficient responses to the problem. For the Congress, this means that there are a number of major policy considerations which require attention prior to a potentially serious increase in computer crime. Prior to discussing policy options in the last section of this report, several of the most important policy considerations are discussed below.

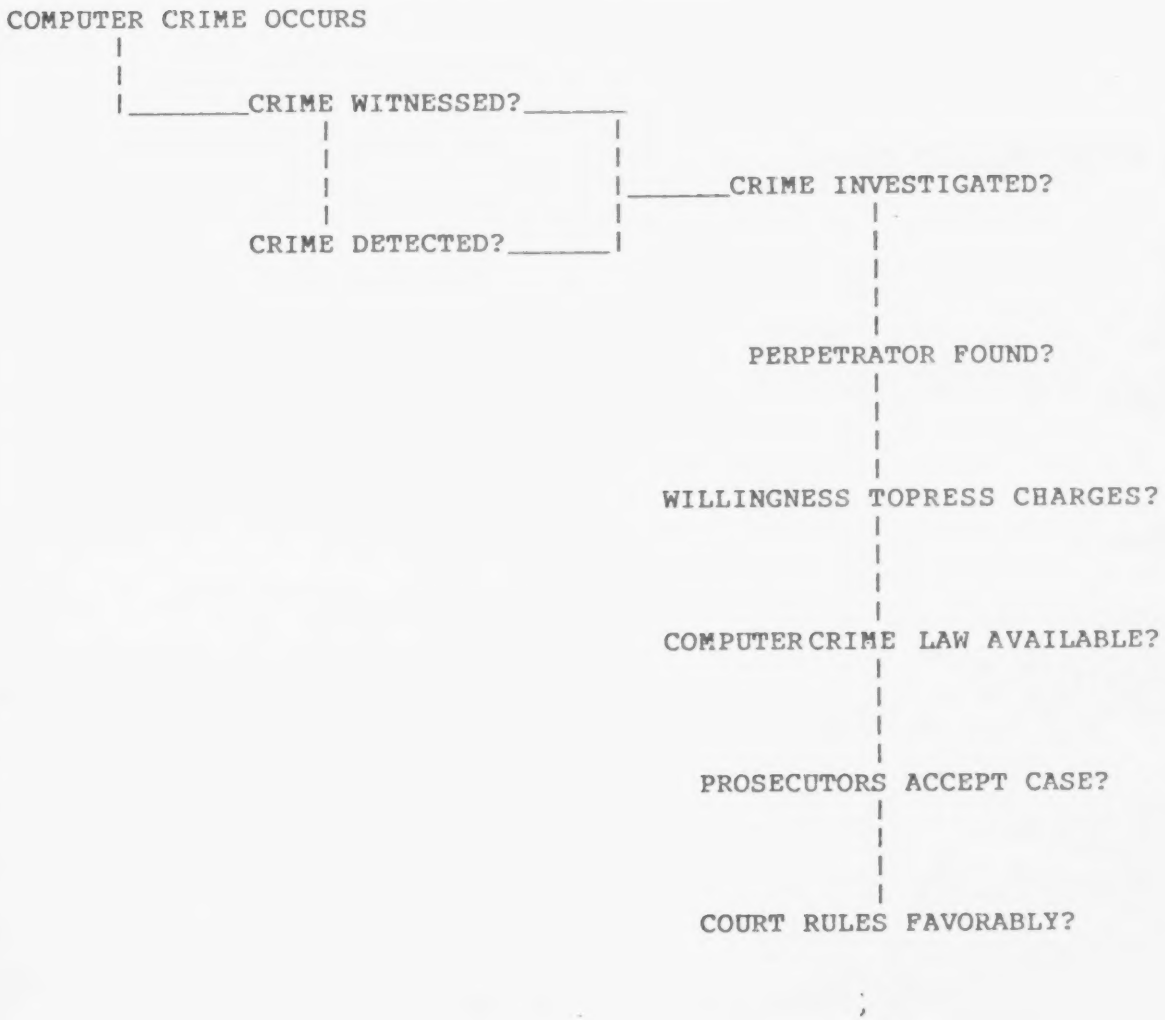
Difficulties in the Development of Technologically Relevant Law

As discussed in the paper, there is a lack of consensus about many of the most basic definitions and approaches required for an effective computer crime bill. As it now exists, formulating computer crime legislation tends to be done in piecemeal fashion with limited attempts to coordinate the variety of issues falling under that general category. For example, it may be that separate efforts being undertaken on software piracy, copyright revisions, revisions of the criminal code, privacy and data protection, and other problem areas might at a minimum be coordinated and reviewed for consistency. Additionally, there have been suggestions that some consideration be given to a uniform state law be drafted by a body such as the National

Conference of Commissioners on Uniform State Laws. [Burk] Such an effort on the Federal level or a joint state-Federal effort might be quite appropriate.

Beyond this, there has been limited discussion of what would be required or necessary in order to implement the legislation in an effective manner. Law enforcement and agency managers tend not to be prepared to respond to computer crime in any different fashion after the development of a computer crime law than before its establishment. The sophistication involved in understanding what computer crime is and how to respond to it will require a great amount of training and assistance in order for the law to be used. Since most crimes come to the attention of law enforcement authorities either when they happen to be on the scene of the crime or through reports from victims or witnesses, both law enforcement and management personnel are going to have to be alerted to the requirements for handling cases. Several of the most prominent problem areas in this regard are shown in the following chart.

MAJOR EVENTS IN THE INVESTIGATION AND PROSECUTION OF A COMPUTER CRIME



All of these can be seen as points at which computer crimes will get winnowed out of the system, not being treated according to the ideal presented in the legislation. The nature of the criminal justice system and the various structural factors which affect whether a case is ever brought to public attention or moved through judicial processing are considerations which will affect how successfully the Government will be able to respond to computer crime.

The area of computer crime legislation is so new that there are a number of important questions which require attention. In order to meet the technological developments of computer crime, both the Government and the private sector need to attend to a variety of new issues.

Establishing Appropriate Legal Responses and Alternative Strategies for Controlling Computer Crime

The limitations of legislative responses to computer crime is another area of relevance. A growing body of research in the sociology of law suggests that there are serious limits to how responsive the law can be in controlling certain social problems. This literature points to the limits of developing sufficient resources and the problems of organizing to control behaviors. The formal structures of social control are often much less successful in changing behaviors than are more informal efforts on the part of peers and other influences.

While law on computer crime may be necessary, it may not serve deterrence purposes unless there is knowledge of what are

the perceptions that computer criminals have about costs and benefits. Additionally, the law will be marshalled after the act of computer crime has been committed and, as indicated in a previous section, the difficulties of detecting these crimes and gaining support from organizations to press charges is very difficult.

What might also be necessary to respond to computer crime is the consideration of alternative responses. There are, for example, certain perquisites in many offices which allow an employee to take home pens, pencils, and paper without this being considered stealing. It is unclear how this has translated into the perquisites of the computerized office. Potentially, employees may feel that using a computer for personal business, taking spare disks, and making copies of programs are the equivalent of the pens, pencils, and paper in the manual office. There is a need to clarify what is and what is not appropriate in the computerized environment.

Rather than concentrate upon the law as a reaction to computer crime, it is possible to develop a series of strategies which are more proactive. Based upon work in the area of white collar crime, the following exhibit provides a suggested model: [Reiss and Biderman]

MODEL OF ARCHETYPICAL REGULATORY ENFORCEMENT AGENCY FOR DETECTING VIOLATIONS

MOBILIZATION STRATEGIES	ENVIRONMENT	
	INTERNAL	EXTERNAL
PROACTIVE	Internal audits of records,practices, etc. Internal inspections by monitors, test, etc.	Reporting requirements submitted by agencies, self reporting of violation required, audits Monitoring systems to detect violations, inspection systems to detect violations
REACTIVE	Investigation of complaints arising internal or external on pesonnel Referral for criminal prosecution	Complaint investigation procedures on external referrals under agency mandate Referral for criminal prosecution

This model provides an alternative strategy to typical computer crime efforts and offers a means by which self-policing efforts on the part of agencies can be structured.

In summary, the problems of computer crime will continue and, if information suggested in the developmental model section is correct, the problem will grow even more serious. While the solutions are not to be easily found, it is advantageous that there are efforts to control this form of crime before it has developed over a long period of time. The more quickly attention is paid to the issue, the greater the possiblities of finding solutions. The major policy issues implied by the material covered in this report are discussed in the following section.

POLICY PERSPECTIVES

XI.POLICY PERSPECTIVES ON INFORMATION SECURITY AND COMPUTER CRIME

The Federal Government's information security is not adequate to meet current threats and vulnerabilities or to adequately prepare for potentially more serious future threats and vulnerabilities. What follows is a suggested agenda of items for the Congress to evaluate in seeking to improve the Government's ability to continue the delivery of basic services and the protection of the citizenry. These items call attention to priority areas requiring the attention and support of the Congress in order to increase the development of information security and to offer legislative responses to computer crime. Acceptance of these items would allow the Federal Government to advance in the fight against computer crime and abuse and to create a more sophisticated response to information crime problems.

Four major policy areas have been selected in consultation with OTA staff and expert workshop par ticipants. These four are (a) **GOVERNMENT RESPONSES TO COMPUTER CRIME**, (b) **FEDERAL GOVERNMENT ORGANIZATION FOR INFORMATION SECURITY**, (c) **MICROCOMPUTER SECURITY**, and (d) **INFORMATION SECURITY RISK MANAGEMENT AND RISK ANALYSIS**. Options are listed for each of these major areas, with each option accompanied by brief comments. It should be noted that there are overlaps in the areas being discussed and certain policy options might well apply to one or more particular topics.

1. POLICY: GOVERNMENT RESPONSES TO COMPUTER CRIME

This report has contained information on the problems involved in establishing effective responses to computer crime. Government responses to the problem have been limited by difficult issues of defining basic technical concepts in appropriate legal fashion and the nature of computer crime which makes it difficult to gain the cooperation of victimized organizations. At present, the potential for serious computer crimes against Government as well as private sector systems appears to have overwhelmed limited security resources and prevention efforts. The near future expansion in the extent, nature, and seriousness of computer crime suggests that there is a need for the Congress as well as the states to act in a concerted effort to control the problem. Among the major policy considerations are computer crime legislation and improvements in computer crime detection and prevention efforts.

POLICY ISSUE I: COMPUTER CRIME LEGISLATION

There is a need for some legislative responses to computer crime, which can serve to assist law enforcement personnel, provide a deterrent message to potential perpetrators, and to protect the general public. There are four general response categories available to the Congress. Regardless of which option or combination of options might be selected, computer crime can most effectively be addressed legislatively by attention to fundamental concepts including determination of the appropriateness of the Federal role, updating of definitions of information technology, consideration of appropriate deterrence

and punishments, appraisal of prosecutorial requirements, establishment of appropriate rules of evidence, and appreciation of detection difficulties.

OPTION A: MAKE NO CHANGES IN EXISTING LAW BUT REQUIRE THAT COMPUTER CRIME BECOMES A LAW ENFORCEMENT PRIORITY. This would make computer crime a higher priority than may now exist among Federal law enforcement agencies and raise Federal law enforcement officials' interest in developing computer crime prevention and investigation programs. As with white collar crime in general, computer crime often involves complex transactions requiring specially trained law enforcement personnel. The success of economic crime units may provide some models for development of computer crime programs. Coordination between Federal and state law enforcement officials regarding the needs for specialized computer crime legislation and technical support for certain investigations would reinforce the usefulness of existing laws.

OPTION B: REVISE EXISTING LAWS AND REGULATIONS TO COVER COMPUTER CRIME ISSUES. Certain current laws relating to financial crimes, privacy, national security, and trespass may may not include sufficient language to cover computer crime. Basic definitions of property and data may require revision as one means of updating existing legislation. This option builds upon the strengths of established legislation and established operating procedures of functioning Federal agencies concerned with financial integrity issues while also creating new tools for meeting computer crime.

OPTION C: CREATE NEW LEGISLATION SPECIFICALLY RELATING TO COMPUTER CRIME. This "clean slate" approach would allow Congress to directly address computer crime with a perspective and legal language developed specifically around that issue. This approach would provide the Congress with an opportunity to meet the problem of computer crime de novo, with consideration given to the approaches to the problem which are considered as most appropriate. Current Congressional legislative proposals differ in terms of how computers and telecommunications systems are defined, how computer crimes can be interpreted, and various approaches to setting punishment limits. These various approaches provide an opportunity for the Congress to establish agreed upon responses to the problem and to develop new legislation to meet the new technological problems of computer crime.

OPTION D: CREATE LEGISLATION WHICH INCLUDES COMPUTER CRIME AS PART OF A LARGER COORDINATED INFORMATION TECHNOLOGY LEGISLATIVE REVIEW. This approach would view computer crime within a framework of information/technology problems, requiring attention to the larger issue of "new technology and old law." In this option, Congress could attempt to establish fundamental laws indicating the Government's perspectives on emerging technology-related matters as intellectual property, privacy and civil liberties, restrictions on surveillance, copyrights and patents, trade secret protections, software piracy, and other areas which require Congressional interpretation and response. Within this perspective, computer or information crime might be

interpreted less as a crime, per se, and more as a technological issue requiring interpretation of ownership of property and authorization requirements over information sources.

POLICY ISSUE 2: COMPUTER CRIME DETECTION AND PREVENTION

There is a need for the Congress to support efforts at improving computer crime detection and investigation. At present, many agencies suffer from a lack of detection and monitoring devices and skilled investigative personnel. Research indicates that computer crimes are almost as likely to be detected by auditing or security personnel as by a chance occurence, such as a co-worker tracking down a suspicious transaction or a client complaint pointing to an agency fraud. This suggests that there may be serious limitations on the state-of-the-art of computer crime detection and that there is a need to increase detection and prevention efforts. Computer crime detection is at a primitive level of development and there are relatively few individuals capable of providing service to agencies. Very basic work on developing detection approaches is required before agencies will be able to support Federal information security efforts. Among the major options are development of fundamental research, mandating more extensive agency prevention, detection, and reporting requirements, designating a lead agency for these efforts, and encouraging computer and telecommunications manufacturers to strength the security of their products.

OPTION A: SUPPORT, REQUIRE, AND/OR FUND BASIC RESEARCH ON CRITICAL COMPUTER CRIME PROBLEMS. Among the fundamental topics for which there is either quite limited information or the need for development of models are computer crime causality and etiology, detection and investigation procedures, computer security awareness training for non-technical personnel, and risk analysis. Congress might approach this option by stating its interest in such research, drawing upon the resources of existing research centers on computer security-related topics, including the National Bureau of Standards, the Department of Defense, NSA, the Bureau of Justice Statistics of the Department of Justice, the Office of Technology Assessment, the General Accounting Office, the Inspectors General/PCIE program, and the National Science Foundation. Joint work between these agencies and the private sector or some form of national commission might be considered, as suggested by some members of Congress.

OPTION B: MANDATE MORE EXTENSIVE AGENCY PREVENTION, DETECTION, AND REPORTING EFFORTS. This may require more specialized personnel, greater security awareness training, and more involved and supportive management. It is clear from GAO reports and other investigations that agencies have not been adequately or appropriately required to support information security efforts. Agency managers have not fully understood the fundamental importance of information security. Given the many daily responsiblities and requirements they must face, different and more appropriate management requirements for information security will be needed in order to achieve proactive rather than

reactive responses. This may be established by means of a national policy for information security and/or for expansion of the work of the inspectors general program with the PCIE to vigorously find computer crime, to interview perpetrators, and to establish security throughout a system's life cycle.

OPTION C: DESIGNATE A LEAD AGENCY FOR DETECTION AND INVESTIGATION EFFORTS. This would involve the development of coordinating mechanism for the sharing of information and approaches to computer crime detection, the setting of uniform standards for identification and reporting of computer crime, and development of improvements in the uses of technology for detection (such as the use of expert systems for crime pattern recognition now being developed by the FBI). This option would provide a greater efficiency of resources in combatting computer crime and the development of model programs and approaches. Additionally, it might provide a "flying squad" of detection and investigatory experts which would be available for assistance to agencies, such as found with the Royal Canadian Mounted Police. Training and development efforts established by the FBI at Quantico, the Federal Law Enforcement Training Center at Glynco, Georgia, and the collection of a data base of Federal computer crime cases by the inspectors general could be supported by this Congressional effort.

OPTION D: ENCOURAGE COMPUTER AND TELECOMMUNICATIONS MANUFACTURERS TO STRENGTHEN ACCESS CONTROLS AND OTHER FORMS OF COMPUTER SECURITY. This encouragement of "built-in" security within systems has already been undertaken by various Government programs, particularly with military agencies. The DoD Computer Security Center's Product Evaluation Program and TEMPEST programs provide some of this encouragement. These efforts, however, may not meet the security needs of the majority of civilian agencies. Congress may have to consider what types of inducements might be required in order to obtain this type of cooperation from the manufacturers. Efforts to strengthen access controls of equipment need to be accompanied by Federal Government efforts to "build-in" security during early stages of the development of agency systems and to gain agency management's acceptance of the important of instituting access control rules.

2. FEDERAL GOVERNMENT ORGANIZATION FOR INFORMATION SECURITY

Information security can be characterized as a cross-cutting issue, affecting a variety of agencies of the Government and committees of the Congress. The variety of technologies involved and the unprecedented types of problems raised may require new organizations and efforts to establish appropriate Federal Government information security efforts. Traditional early warnings systems which bring problems to the attention of the Congress or agencies may not be sufficient for such fast moving

problems as computer crime. Traditional means of establishing agency responsibility over personnel and equipment may be challenged by information security requirements. Traditional means of responding to white collar crimes, financial abuses, integrity requirements, and Governmental efficiency may have to be reviewed in order to meet the growing computerization of Government. Among the major options are required coordination or centralization of information security responsibilities, establishment of programs to overcome the implementation obstacles to agency information security efforts, evaluation of NSDD 145 and civilian/military information security programs, and inquiries concerning the reliability of Government information systems and potential threats causing overdependence, possibly affecting the delivery of basic Governmental services.

OPTION A: REQUIRE COORDINATION OR CENTRALIZATION OF INFORMATION SECURITY RESPONSIBILITIES. The Federal Government's information security has been characterized as a "muddle." The implications of this muddle is that the Government appears to be unprepared to meet today's security problem at a time when the problem continues to grow. Islands of information security exist within a sea of unsecured systems, unprotected data, and a lack of direction from the Congress or the Administration. Agency administrators and security managers may not know where to turn for direction or assistance. Previous Government efforts to coordinate or regularize information security have often failed due to a combination of lead agency insufficiencies, rapid changes in technology, and bureaucratic infighting. Congress may

wish to make some fundamental decisions on how computer and telecommunications security should best be structured for the Federal Government, particularly civilian agencies.

Foremost among the considerations involved with this option are whether to structure this coordination or centralization through (a) one super information security agency which has Government-wide responsibilities for technical and personnel security matters, (b) separate super information security agencies with technical and personnel security responsibilities for the civilian and military agencies, (c) a regulatory-type agency with responsibility for developing security guidelines and requirements for agencies, (d) coordinating mechanisms which require certain baseline measures to be met by agencies while allowing agency management personnel to define their own security requirements and approaches, (e) a central source for information security programs, evaluations, tools, purchasing guides, and other assistance but without any standards-setting responsibilities. Related to the selection of options are Congressional consideration of its support for proposed budget cuts which may effectively remove the National Bureau of Standards from any further computer security efforts on behalf of civilian agencies as well as the private sector, the implications of NSDD 145 for NSA's role in both civilian and military agency security, and the lack of skilled security experts outside of certain agency centers.

OPTION B: ESTABLISH THE MEANS TO OVERCOME THE IMPLEMENTATION OBSTACLES TO AGENCY INFORMATION SECURITY EFFORTS. Obstacles to information security implementation have been cited in the body of this report. These include the lack of central leadership to provide a clear and well defined set of national goals to protect computer and communications systems, unclear determination of the distinct responsibilities of various lead agencies, lack of strong national leadership, failure of agency senior management to treat information security as a serious problem, and deficiencies in defining reasonable levels of protection for civilian agencies. Many of these obstacles could be affected by Congressional decisions on other options, such as whether information security will be coordinated or centralized and, if so, what form that effort might take. Congress may also wish to establish a set of national goals for information security which will balance the possible contradictions between the broad social goals of the Privacy Act of 1974 and FOIA with the design and implementation of information security policies. Finally, senior management have to balance a number of demands and requirements, including the need to balance productivity and protection of their agency's system. Guidance on how to increase protection while continuing production would provide vital information to those managers.

OPTION C: EVALUATE NSDD 145. NSDD 145 is a leading current policy document concerning information security. It provides an operating structure and a set of information security objectives which have been created to overcome past Government efforts at protecting systems. At least one committee of Congress has raised questions about the Directive, particularly the role of NSA. NSA has achieved significant expertise in a variety of information security specialties. Whether and how this expertise will be used in an overall Federal Government information security program continues to be a controversial matter.

> First, the extent of NSA's role with regard to security of unclassified data in federal government computers is unclear. Second, the relationships between NSA and unclassified private sector communications and computer security measures are uncertain. The 1984 Presidential Directive deals only with protection of information for national security reasons, not with other private considerations for either government or private sector data. The intent is to offer help to the private sector on a voluntary basis in protecting unclassified information. Therefore, a proposal that the U. S. Government support private research and development efforts on a low-cost security telephone system is of special interest to the Committee. [**U. S. Senate Select Committee on Intelligence**]

Working groups formed to implement NSDD 145 are meeting to determine the best means of achieving this overall national approach. Congress may wish to review the Directive and to provide its view of appropriate ways to classify, protect, and distribute information, particularly involving several major civilian agencies which were not included under the specifications of the Directive and which do not appear to be participating in the deliberations of the working groups.

OPTION D: INQUIRE ABOUT THE RELIABILITY OF GOVERNMENT INFORMATION SYSTEMS AND THE POTENTIAL THREATS OF OVERDEPENDENCE. The national existence and the delivery of vital Government services may be threatened by risks and vulnerabilities of information systems. For networks in particular, there are "three R's" of reliability, e.g., robustness, or resistance to damage and abnormal stress; ruggedness, or ability to continue functioning at least partially in the presence of damage and stress; and resilience, or the capacity for rapid and complete return to normal operation following damage and stress. [**The Center for Strategic and International Studies**] Contingency planning provides the basis for undertaking and implementing basic preventive and corrective measures. Yet, according to GAO and other studies, contingency planning tends to be inadequate in the majority of Government agencies, and specific measures of physical protection, redundancy, and stockpiling may not be sufficient. Unless more attention is paid by agencies to reducing risks associated with reliability factors, the rapid computerization of the Government may turn out to be an overdependence on technology which is hostage to various "Acts of God" as well as sabotage. Congress may play an important role by raising questions about the potential for overdependence and the adequacy of risk reduction and reliability controls.

3. POLICY: MICROCOMPUTER SECURITY

The rapid increase of microcomputers within the Federal Government has led to special security problems. The microcomputer environment has several distinct characteristics which differentiate it from mainframe or minicomputer environments. Microcomputers tend to have inexperienced users, ineffective internal controls, limited data protection, increased physical accessibility, lack of backup of data, outdated contingency planning, and, when networks of micros and mainframes are operating, relatively open access to data. In that sense, microcomputers have created an increased security problem for the Government, adding to the complexity of improving information security. While the microcomputer security problem continues to unfold and experts are presently grappling with basic security responses, certain options available to the Congress are evident. These options include requiring security considerations to be incorporated within agency microcomputer purchase plans, setting of standards for how security might require limitations on microcomputer configurations and usage patterns, support for the development of microcomputer security product evaluations and models for improved security awareness training, and requiring increased end user security responsibilities and protections.

OPTION A: REQUIRE SECURITY CONSIDERATIONS TO BE INCORPORATED WITHIN AGENCY MICROCOMPUTER PURCHASE PLANS. Often, much more attention tends to be paid to the purchase of equipment than to the security implications of the equipment. The establishment of agency purchase procedures and the centralization of Government computer stores have developed rapidly, with relatively little attention to incorporating security requirements within those developments. Purchase requirements could be modified by agencies and by GSA. A security impact statement regulation might be established, requiring that a report must be prepared prior to allowing any major purchase and/or enhancement of computers, particularly microcomputers. This security impact statement would allow agency managers to ascertain the security implications of a proposed system and establish how appropriate security plans to meet those implications will be put into operation.

OPTION B: SET STANDARDS FOR HOW SECURITY MIGHT REQUIRE LIMITATIONS ON MICROCOMPUTER CONFIGURATIONS AND USAGE PATTERNS. Security may require revision of certain existing legislation which seeks to increase Government productivity and use of equipment. Certain agency functions may require microcomputers to be "powered down" so that security can be maximized. This might include increased use of "dumb" terminals, restrictions on access to certain data or files, redundant equipment, and other

means of restricting the productivity of computers. These more restrictive uses of microcomputers will reinforce the security principles of separation of duties and the need to know. This is not a move to limit Government use of microcomputers but a means of controlling how those micros are used in secure fashion.

OPTION C: SUPPORT THE DEVELOPMENT OF MICROSECURITY PRODUCT EVALUATIONS AND MODELS FOR IMPROVED SECURITY AWARENESS AND TRAINING EFFORTS BY AGENCIES. Microcomputer security is receiving the attention of vendors with more products suddenly becoming available. The plethora of microcomputer security products have, however, led to a need for some product review and evaluation so that agencies can make educated decisions on their security purchases. The Product Evaluation Program of the DoD Computer Security provides aspects of that approach, although the criteria for evaluation are based on the Trusted Computer System, which may not be applicable or necessary for the majority of civilian agency needs. The National Bureau of Standards has established an information security products database, which provides information on basic manufacturer specifications and application information for Government agencies and the private sector. They have also recently released a report on microcomputer security. Much more work is needed in security product development and evaluation as well as the security awareness and training area . This latter area has received limited attention from security experts and continues to be one of the weakest aspects of security implementation in agencies. Without improvements in security awareness and training, the

"peopleware" aspect of information security will be limited and "technicalware" approaches will continue to be limited in their ability to control the human behavior of computer crime. Training and awareness models might be sought from the fields of human behavior, training, education, and organizational behavior. Models based upon these perspectives might allow security to be incorporated into the operating perspectives of agencies and end users.

OPTION D: INCREASE END USER SECURITY RESPONSIBILITIES AND PROTECTIONS. The end user has now been placed in the position as one of the major security officials in Government. The clerk typist of yesterday is today's data entry person, working with computers in environments where security may be lacking and supervision may be inadequate. Previously, the data center had been able to provide aspects of security to user agencies. The microcomputer has changed much of this, requiring end users to become actively involved in the security, data integrity and backup, contingency planning, environmental control, and physical protection of their equipment and data. Without sufficient training and awareness as well as agency-developed security policies, procedures, and equipment, the end user may be incapable of following quite basic security operations or supporting agency security efforts. In order to function, this option may require acceptance by Congress of other options presented in this section of the paper as well as concerted efforts by agencies directing security messages to end users. In addition, the required creation and distribution of data

ownership policies could allow end users to gain knowledge of what their responsibilities are, while privacy policies could provide them with a means of understanding how they as well as the public are protected from unauthorized data distribution.

4. POLICY: INFORMATION SECURITY RISK MANAGEMENT AND RISK ANALYSIS

Risk management includes a range of actions taken to avoid, minimize, reduce, limit, or otherwise control the degree of exposure to risk situations or the magnitude of adverse consequences. Risk analysis, sometimes also called risk assessment, is the process of identifying, characterizing, quantifying or qualifying, and evaluating the risk, cost, and benefit factors associated with a proposed action or condition. While both risk management and risk analysis are required in information security programs, reviews of agencies indicate limited attention to these efforts. Congress can provide assistance in creating agency interest and active involvement with attempts to limit risks within their information systems. Among the major policy options are requiring that risk analysis be incorporated within early phases of system development life cycles and support for the transfer of risk analysis knowledge and techniques developed for other aspects of Government uses.

OPTION A: REQUIRE THAT RISK ANALYSIS BE INCORPORATED WITHIN EARLY PHASES OF SYSTEM DEVELOPMENT. Risk management and risk analysis often is applied after a system is in place and security concerns are raised. A more cost-effective approach is to build in risk evaluations and risk reduction decisions during all phases of a system development life cycle. This provides the possibility for security to be integrated into technical and procedural aspects. The PCIE is attempting to increase the effective audit review of automated information systems under development and to insure that new systems are installed with adequate internal controls, security features, and audit trails. A responsibility matrix has been developed listing the roles and responsibilities of key actors and the documentation considered as necessary throughout a systems life cycle. A generalized audit guide is under preparation, outlining an approach to reviewing systems under development and enumerating key areas of audit concern. This PCIE project, and similar projects in various agencies, may provide basic information which Congress may wish to use as Government-wide measures for establishing built-in security during development work.

OPTION B: SUPPORT THE TRANSFER OF RISK ANALYSIS KNOWLEDGE AND TECHNIQUES DEVELOPED FOR OTHER ASPECTS OF GOVERNMENT USE. Risk analysis continues to be relied upon as a major tool for determining an agency's risks and vulnerabilities. Information security risk analyses have a number of limitations and restrictions, creating the need for more developed models and approaches to determining risk and vulnerability information.

Recent work by NBS, the Air Force, and the private sector has been quite productive and there are some experts who have suggested the availablility of usable information security risk analysis products in the near future. There is, however, a repository of basic information on risk analysis which appears to have been neglected by those concerned with information security. That is the body of knowledge developed by other agencies for such risk areas as regulatory reviews, estimations of health complications, evaluations of foods and drugs, and other scientific and health reviews. The National Science Foundation has a program on risk assessment and several major studies have been developed which provide insights into aspects of the process. It may well be that information on risk analysis developed for a regulatory agency, for example, could be modified for information security applications. Congress can assist the information security effort by supporting joint efforts on the development of risk analysis approaches and other forms of coordinating and sharing of technical resources. Included in such an effort may be funding for artificial intelligence applications, such as expert systems-based risk analysis techniques.

SUMMARY

This assortment of policy options provides the Congress with a menu of choices in strengthening the nation's information security. The problems of previous Governmental efforts to establish information security have been detailed in this report. The success of future information security efforts will largely depend upon how Congress is able to grapple with quite complex technical and human behavior issues and provide direction to Federal agencies as well as the nation at large.

FOOTNOTES

Batelle Laboratories , Columbus, Ohio. Study for a U. S. House Committee as reported in "Greenbacks May Get a Face Lift," **Security Word**, December 1984, p. 11.

Louise Giovane Becker, **Computer Security: An Overview of National Concerns and Challenges**, Congressional Research Service, February 3, 1983 (TK 7885 E).

Louise Giovane Becker, **Privacy: Information Technology Implications**, Congressional Research Service Issue Brief Number 1B 74105, updated 21 March 1975.

Joel Best and David F. Luckenbill, **Organizing Deviance**, Englewood Cliffs, N.J.: Prentice-Hall Inc., 1982.

Daniel R. Burk, "The Philosophies of Computer Crime Legislation: An Editorial Collection," **Computer Law Reporter**, Vol. 3, No. 3, November 1984.

Robert Campbell, "Computer Security as a Management Issue", in **Advances in Computer Security Management**, Vol. 2, M. M. Wofsey (Ed.), New York: John Wiley & Sons, Inc., 1983, p. 35.

John M. Carroll, **Managing Risk**, Boston: Butterworth, 1984.

Center for Strategic and International Studies, **America's Hidden Vulnerabilities: Crisis Management in a Society of Networks**, Washington, D.C.: Georgetown University, 1984.

Committee on Multilevel Data Management Security Air Force Studies Board, Commission on Engineering and Technical Systems, National Research Council, **Multilevel Data Management Security**, Washington, D.C.: National Academy Press, 1983, pp. 9-10.

Comptroller General of the United States, **Fraud in Government Programs: How Extensive is it and How Can it be Controlled?**, AFMD-81-73, September 30, 1981.

Comptroller General of the United States, **Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economies** (LCD-81-1), November 12, 1980.

Computer and Communications Security and Privacy. A report prepared by the Subcommittee on Transportation, Aviation and Materials and transmitted to the Committee on Science and Technology. U.S. House of Representatives, 98th Congress, 2d Session, April 1984, pp. 28, 30, 198, 199.

Computer Crime: Criminal Justice Resource Manual, Bureau of Justice Statistics, Department of Justice, Washington, D.C., 1979.

Computerworld, July 23, 1984.

D. W. Davies, et al., **Computer Networks and Their Protocols**, Chichester, England: John Wiley & Sons, 1979.

William H. Dutton and Robert G. Meadow, **Public Perspectives on Government Information Technology**, Draft Report for OTA, December 1984, p. 38.

Robert W. Edwards, **Data Processing: Security and Control**, Pennsauken, N.J.: Auerbach Publishers Inc., 1983.

Samantha Fordyce, "Computer Security: A Current Assessment," **Computers & Security** 1 (January 1982), p. 12.

Roy Freed, "Legal Interests Related to Software Programs." To be published in **Jurimetrics Journal**, Vol. 25, #3, 1985.

Cyrus F. Gibson and Richard L. Nolan, "Managing the Four Stages of EDP Growth", reprinted in Lynn M. Salerno, (Ed.), **Catching Up with the Computer Revolution**, New York: John Wiley & Sons Inc., 1983, pp. 25-43.

Elizabeth A. Glynn, "Computer Abuse: The Emerging Crime and the Need for Legislation," **Fordham Urban Law Review**, Vol. 12, No. 1, 1983-1984: pp. 73-110.

Hearings on S. 240: The Federal Computer Systems Protection Act of 1979. Before the Subcommittee on Criminal Justice of the Senate Judiciary Committee, 96th Congress, 2d session, 1,15 (1980). Statement of J. D. McFarlane.

Bruce Jackson, **A Thief's Primer**, New York: The MacMillan Company, 1969.

Kenneth L. Kittleberger, "Scope of Computer Security Problems", in M. M. Wofsey (Ed.), **Advances in Computer Security Management**, Vol. 2, New York: John Wiley & Sons, 1983, pp. 1-24.

Robert H. Kupperman, **Facing Tomorrow's Terrorist Incident Today**, Law Enforcement Assistance Administration, October 1977, Technical Appendix.

Richard P. Kusserow, **Computer-Related Fraud and Abuse in Government Agencies**, Inspector General Office, HHS, 1983.

Peter Letkemann, **Crime as Work**, Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1973.

John F. Maxfield, **Computer Bulletin Boards and the Hacker Problem**, Detroit: BOARDSCAN, 1984.

National Communications Security Committee, **Computer and Telecommunications Security,** Report of the Working Group on Computer Security, July 1981, pp. 48, 51.

National Security Decision Directive 145 (NSDD 145), **National Policy on Telecommunications and Automated Information Systems Security,** September 17, 1984.

Susan Nycum, "The Criminal Law Aspects of Computer Abuse: Part II: Federal Criminal Code," **Rutgers J. Computers & L.**. 297, pp. 305-322 (1976).

Susan H. Nycum and Daniel L. Appelman, **Legal and Managerial Approaches to Intrusion Protection.** A paper presented at the NSF Workshop on Protection of Computer Systems and Software, October 19, 1984.

Proceedings of the Seminar on the DoD Computer Security Initiative Program, National Bureau of Standards, Gaithersburg, MD. 17-18 July, 1979.

Albert J. Reiss, Jr. and Albert D. Biderman, **Data Sources on White Collar Law Breaking,** U. S. Department of Justice, National Institute of Justice, September 1980, p. 112.

Timothy Saltmarsh and Peter S. Browne, "Data Processing-Risk Assessment", in M. M. Wofsey (Ed.), **Advances in Computer Security Management,** Vol. 2, New York: John Wiley & Sons Ltd., 1983, pp. 106-114.

Edwin M. Schur, **The Politics of Deviance,** Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1980.

Sanford Sherizen, **How to Protect Your Computer,** New York: American Management Associations, 1984.

Paul Slovic, et al., "Facts vs. Fears: Understanding Perceived Risk," presentation at the Royal Society, 12 November 1980. As cited in Adrian Norman, **Computer Insecurity,** New York: Chapman and Hall, 1983.

Erwin O. Smigel, "Public Attitudes Toward Stealing as Related to the Size of the Victim Organization," **American Sociological Review,** Vol. 21, No. 3, June 1956.

Edwin Sutherland, **The Professional Thief,** Chicago: The University of Chicago Press, 1937.

Gresham Sykes, **The Future of Crime,** Rockville, MD.: NIMH, Center for Studies of Crime and Delinquency, 1980.

John D. Tangney, **History of Protection in Computer Systems,** Bedford, MA.: MITRE, 1980.

Frederick G. Tompkins, **Guidelines for Developing NASA ADP Security Risk Management Plans**, McLean, VA.: MITRE, 1983.

Frederick G. Tompkins, **Guidelines for Developing NASA ADP Security Risk Reduction Decision Studies**, McLean, VA.: MITRE, 1983.

U. S. Senate. **Report of the Select Committee on Intelligence**, 1984, p. 35.

U. S. Department of Labor, Employment and Training Administration, Unemployment Insurance Service, **Risk Analysis Guidance Document**, Washington, D.C. 1982.

U. S. Senate Committee on the Judiciary. Subcommittee on Criminal Justice. **Computer System Protection Act of 1979. Hearings on S. 240.** 96th Congress, 2d session. Hearings held on February 28, 1980.

Victor C. Walling, Jr., et al., **Impacts of Federal Policy Options for Nonmilitary Cryptography**, Washington, D.C.: NTIA, 1981.

Leslie Wharton, "Legislative Issues in Computer Crime," **Harvard Journal on Legislation**, Vol. 21, Winter 1984: pp. 239-254.